```
Set     Items   Description
S1     701620   WIRELESS? OR WIRE()LESS? OR RADIO? OR CELLULAR? OR MOBILE?
             OR WAP? ? OR WLAN? ? OR CELLPHONE?
S2     180859   PLURAL? OR SEVERAL? OR MULTIPL? OR MULTIT? OR NUMEROUS? OR
             MANY OR CLUSTER? OR SET OR SETS
S3      65977   ARRAY? OR ASSORTMENT? OR GROUP? OR COLLECTION? OR ASSEMBLY?
S4       4411   (AUTHENTICAT? OR AUTHORIZ? OR AUTHORIS? OR VERIF? OR CERTI-
             F? OR IDENTIF? OR VALIDAT? OR SECUR?)(3N)(PREFERENC? OR PROTO-
             COL? OR IDENTIT? OR ID OR PASSKEY? OR PASSWORD?)
S5        262   (CRYPT? OR ENCRYPT? OR DECRYPT? OR ENCIPHER? OR DECIPHER?)-
             (3N)(HANDSHAK? OR HAND()SHAK? OR IDENTIT? OR ID OR PASSKEY? OR
              PASSWORD? OR PROTOCOL?)
S6       2899   CHAP OR EAP OR PAP OR SPAP OR DES OR RADIUS OR SKEY OR S()-
             KEY OR TACACS OR MSCHAP? OR SKID? ?
S7         47   (CONFIRM? OR CORROBORAT?)()(IDENTIT? OR ID OR PASSKEY? OR -
             PASSWORD? OR PROTOCOL? OR HANDSHAK? OR HAND()SHAK?)
S8      53553   HUB? ? OR ACCESS?()POINT? OR BASE()STATION? OR BASESTATION?
              OR (CELL? OR HANDOFF? OR HAND?()OFF)()(TOWER? OR BEACON?)
S9       7523   GATEWAY? OR GATE()WAY? ? OR ROUTER? ? OR (NET? ? OR NETWOR-
             K?)()(SWITCH? OR HANDOFF? OR HAND?()OFF) OR ACCESS?()SERVER?
S10    144862   SPECIFY? OR SPECIFIE? OR PREFER?  OR SELECT? OR CHOOS? OR -
             CHOIC?
S11    136029   ELECT? OR DESIGNAT? OR DISCRIMINAT? OR ASSIGN? OR PICK?  OR
              OPT OR OPTS OR OPTED OR OPTING
S12     48508   OPTION? OR SCHEDUL? OR ACTUAT? OR EXECUT?
S13    234514   SINGLE? OR UNIQUE? OR SPECIF? OR PARTICULAR? OR INDIVIDUAL?
              OR LONE? OR SINGULAR? OR ONE
S14    219506   INDEPEND? OR DISTINCT? OR SPECIFIC? OR CERTAIN? OR DEFINIT?
              OR PRECIS?
S15    140953   EXCLUSIV? OR EACH? OR TARGET? OR DEDICAT? OR DEPENDEN?
S16    229192   IC=(H04Q? OR H04M? OR G06F? OR H04L?)
S17    297430   MC=(W01? OR T01? OR W03? OR W04? OR W02?)
S18        22   S1 AND S8:S9(5N)S10:S12 AND S13:S15(5N)S4:S7
S19         7   S1 AND S2:S3(5N)S4:S7 AND S8:S9(7N)S10:S12 AND S8:S12(7N)S-
             13:S15
S20       732   S1 AND S4:S7 AND S8:S9 AND S10:S15 AND S16:S17
S21       266   S20 AND S10:S12 AND S13:S15
S22       187   S21 AND (S2:S3 OR S13:S15)(10N)(S1 OR S4:S7)
S23        27   S18:S19
S24        27   IDPAT (sorted in duplicate/non-duplicate order)
S25       164   S22 NOT S23
S26        50   S25 AND AC=US/PR
S27        24   S26 AND AY=(1970:2000)/PR
S28       114   S25 NOT S26
S29        32   S28 AND PY=1970:2000
S30        56   S27 OR S29
S31        56   IDPAT (sorted in duplicate/non-duplicate order)
File 347:JAPIO Nov 1976-2005/Oct(Updated 060203)
         (c) 2006 JPO & JAPIO
File 350:Derwent WPIX 1963-2006/UD,UM &UP=200610
         (c) 2006  Thomson Derwent
```

31/3,K/31 (Item 31 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010896874 **Image available**
WPI Acc No: 1996-393825/ **199640**
XRPX Acc No: N96-331882
Access point **for controlling messages between wired and** wireless **communication networks, esp. LANs - has table containing identity and predetermined communication parameters of** each **node in** wireless **network for comparing with information associated with received messages, only transmitting messages which will elicit response**
Patent Assignee: IBM CANADA LTD (IBMC); INT BUSINESS MACHINES CORP (IBMC)
Inventor: BAKER M C; BHATTACHARYA P P; CHEUNG R Y M; KOBO R M; KOLBE E M; NAGHSHINEH M
Number of Countries: 002 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
CA 2137587	A	19960609	CA 2137587	A	19941208	199640	B
US 5570366	A	19961029	US 95443793	A	19950518	199649	
CA 2137587	C	19990323	CA 2137587	A	19941208	199930	

Priority Applications (No Type Date): CA 2137587 A 19941208
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
CA 2137587	A		29	H04L-012/46	
US 5570366	A		16	H04J-003/02	
CA 2137587	C			H04L-012/46	

Access point **for controlling messages between wired and** wireless **communication networks, esp. LANs...**

...has table containing identity and predetermined communication parameters of each **node in** wireless **network for comparing with information associated with received messages, only transmitting messages which will elicit...**

...Abstract (Basic): The **access point** includes a table which contains the identity of **each** node in the associated **wireless** network and predetermined communication parameters associated with **each** node. Identity and communication parameter information associated with received messages is compared with the corresponding...

...result of the comparison is used to determine whether the message is transmitted to the **wireless** network, transmitting only messages which will elicit a response from **one** of the **wireless** network nodes...

...Pref. the wired and **wireless** networks are LANs and the predetermined communication parameters define destination addresses, **protocol identifiers** and destination names associated with **each** protocol, for **each mobile** terminal associated with the **access point** . The message and table parameters can also be **selectively** compared to allow a desired level of filtering. Pref. table entry information can be transferred between **access points** when a **mobile** terminal moves between **wireless** LANs...

...ADVANTAGE - Ensures messages are only transmitted to **target** stations which will act on them...
...Abstract (Equivalent): In a communications system comprising a **plurality** of wired networks, a **plurality** of **wireless** networks and

an **access point** between **each wireless** network and a wired network, **each** said **access point** controlling the transmission of messages between **one** of said **wireless** networks and **one** of said wired networks, wherein said **access points** control said transmission by performing the following steps...

...creating a table in **each** said **access point** , said table including the identity of **each** node in its associated **wireless** network and predetermined communication parameters associated with **each** node on said associated **wireless** network...

...comparing identity and communication parameter information associated with **each** message received by said **access point** with corresponding information in said table at said **access point** ; and ...

...transmitting, to said associated **wireless** network, only those messages which will be responded to by a node on said associated **wireless** network as determined by comparing said identity and communications parameters in said received message to...

...Title Terms: **WIRELESS** ;

...International Patent Class (Main): **H04L-012/46**

International Patent Class (Additional): **H04Q-007/24** ...

... **H04Q-007/38**

Manual Codes (EPI/S-X): **W01-A06B5A** ...

... **W01-A06C2** ...

... **W01-A06C4** ...

... **W01-A06E1** ...

... **W01-A06G3**

US005570366A

United States Patent [19]

Baker et al.

[11] Patent Number: 5,570,366

[45] Date of Patent: Oct. 29, 1996

[54] **BROADCAST/MULTICAST FILTERING BY THE BRIDGE-BASED ACCESS POINT**

[75] Inventors: **Murray C. Baker**, Toronto; **Roger Y. M. Cheung**, Scarborough, both of Canada; **Partha P. Bhattacharya**, Briarcliff, N.Y.; **Roberto M. Kobo**; **Eduardo M. Kolbe**, both of Campinas, Brazil; **Mahmoud Naghshineh**, Fishkill, N.Y.

[73] Assignee: **International Business Machines Corporation**, Armonk, N.Y.

[21] Appl. No.: **443,793**

[22] Filed: **May 18, 1995**

[30] **Foreign Application Priority Data**

Dec. 8, 1994 [CA] Canada 2137587

[51] **Int. Cl.**[6] **H04J 3/02**

[52] **U.S. Cl.** **370/85.13**; 370/94.1

[58] **Field of Search** 370/85.13, 85.14, 370/85.15, 85.5, 85.7, 85.8, 85.2, 85.3, 85.4, 95.1, 95.2, 95.3, 92, 93, 100.1, 105.1, 110.1, 118, 60, 60.1, 94.1, 94.2, 94.3, 61, 13, 17, 54, 18; 455/3.2, 5.1, 11.1, 15, 53.1, 54.1, 54.2, 56.1, 55.1, 33.2, 58.2, 66, 78, 38.2, 38.3; 348/6, 7, 12; 375/240, 224, 220, 212, 213, 207, 208, 293, 356; 379/58, 60, 63; 340/825.02, 825.05, 825.07, 825.08, 825.15, 825.21, 825.52, 825.47

[56] **References Cited**

U.S. PATENT DOCUMENTS

Re. 28,811	5/1976	Pierce	370/85.4
4,049,906	9/1977	Hafner et al.	370/61
4,081,612	3/1978	Hafner	370/60
5,159,592	10/1992	Perkins	370/85.13
5,276,703	1/1994	Budin et al.	370/93
5,339,316	8/1994	Diepstraten	370/85.13

OTHER PUBLICATIONS

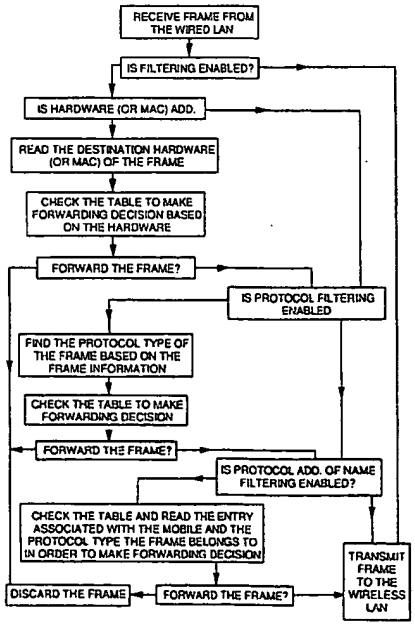
"Extendability Considerations in the Design of the Distributed Computer System (DCS)", Farber et al., pp. 15E-1 to 15E-6.

Primary Examiner—Douglas W. Olms
Assistant Examiner—Dang Ton
Attorney, Agent, or Firm—Joscelyn G. Cockburn

[57] **ABSTRACT**

In communication systems which include high speed wired local area networks (LANs) and low speed wireless LANs, the bandwidth of the wireless LANs can be severely impacted. It has been found that many broadcast or multicast messages which are forwarded to the wireless LANs are not required as the mobile terminals which would receive the messages are not required to act on them. The present invention provides a means and method to filter out unneeded messages so that they do not impact the bandwidth of the wireless network. Each access point for each wireless LAN maintains a table of parameters for each associated mobile terminal in the connected wireless LAN. The parameters in that table are compared to the parameters in message frames received by the access point and only those messages having parameters found in the table are put on the wireless LAN. The level of filtering can be controlled by specifying which parameters are to be used for filtering messages. The tables at each access point are maintained current by moving table entries from access point to access point as mobile terminals move from wireless LAN to wireless LAN and by removing inactive table entries from the table when a predetermined interval of inactivity is encountered and a terminal is determined to be no longer in active contact with the access point.

12 Claims, 8 Drawing Sheets



-continued

```
>
else
  forward the frame
```

It is easy to see how the invention can be extended to other protocol stacks. In general, the access point needs to construct a separate filtering database per protocol stack on which it wishes to apply filtering. The database has a field that uniquely identifies a network node in the wireless network for which a broadcast or multicast data frame is actually intended.

When data frames are received from the slow wireless network, the access point examines the data frame to determine to which protocol stack it belongs. Then the access point checks the corresponding protocol stack's broadcast/multicast filtering database to determine if the unique entry for the source network node is already present. If the entry does not exist, the access point creates it.

When a broadcast or multicast data frame is received from the fast wired network, the access point examines the data frame to determine to which the protocol stack it belongs.

Depending upon the protocol, it finds the Name/Address associated with that protocol included in the frame, then it goes to the table to look for the Name/Address associated with the access point. Then the access point checks the corresponding protocol stack's broadcast/multicast filtering database. Only if the Name/Address was found in the protocol stack's database should the access point forward the frame to the slow wireless network.

If the access point is informed by another access point that the mobile network node has moved to its vicinity and registered with the other access point, the access point will deregister the mobile network node and forward the entries in the protocol stack's broadcast/multicast filtering database that are associated with the mobile network node to the access point with which the mobile terminal is newly registered. The deregistering access point will also delete those entries from the protocol stack's broadcast/multicast filtering database.

Each protocol stack's broadcast/multicast filtering database has an expiry counter associated with each entry in the database. Whenever the access point receives, from the wireless LAN, a broadcast or multicast data frame that belongs to the protocol stack, the access point checks to see if a corresponding entry exists in the protocol stack's broadcast multicast filtering database. If an entry exists, the expiry counter associated with that entry is reset to a predetermined timeout value. When the expiry counter reaches zero, after the predetermined timeout period, the filtering database entry will be deleted unless the mobile network node is still registered with the access point. In that case, the expiry counter is reset to the predetermined timeout value.

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. In a communications system comprising a plurality of wired networks, a plurality of wireless networks and an access point between each wireless network and a wired network, each said access point controlling the transmission of messages between one of said wireless networks and one of said wired networks, wherein said access points control said transmission by performing the following steps:

creating a table in each said access point, said table including the identity of each node in its associated wireless network and predetermined communication parameters associated with each node on said associated wireless network;

comparing identity and communication parameter information associated with each message received by said access point with corresponding information in said table at said access point; and

transmitting, to said associated wireless network, only those messages which will be responded to by a node on said associated wireless network as determined by comparing said identity and communications parameters in said received message to entries in said table.

2. In a communications network including at least one wired network and at least one wireless local area network LAN and at least one access point connecting the at least one wireless LAN to the at least one wired network, a device to control transmission of messages between said at least one wireless LAN and said at least one wired network so as to preserve bandwidth on said at least one wireless LAN, said device comprising:

means for storing a table of predetermined message parameters at the at least one access point;

means for comparing parameters in each message received from the at least one wired network connected to said at least one access point to said parameters stored in said table; and

means for transmitting messages between said at least one wireless LAN and said at least one wired network when said parameters in said each message correspond to message parameters in said table in said at least one access point.

3. In the communications network as defined in claim 2 wherein said at least one wired network includes LANs.

4. In the communications network as defined in claim 2 or claim 3 wherein said communications network includes mobile terminals in said at least one wireless LAN and said predetermined parameters define destination addresses, protocol identifiers and destination names associated with each protocol for each mobile terminal associated with said at least one access point.

5. The communication network system as defined in claim 4 further including means to selectively compare said parameters in said message to said parameters in said table so that a preferred level of filtering of said messages can be selected.

6. The communication network as defined in claim 4 and further including means for transferring table entry information from one access point to a second access point when a mobile terminal moves from a first wireless LAN connected to said one access point to a second wireless LAN connected to said second access point.

7. The communication network as defined in claim 6 wherein said means for transferring transfers said table information directly from said table in said one access point to said table in said second access point.

8. The communication network of claim 6 wherein said means for transferring includes transmitting said table information directly from said mobile terminal to said table in said second access point in response to an indication from said mobile terminal that it requires access to said second access point.

9. In the communications network as defined in claim 5 wherein said at least one access point further includes means for responding to broadcast traffic levels in said wired network to control said level of filtering.

10. In the communications network as defined in claim 1 further including the steps of selecting additional parameters

in said table for comparison with parameters received in said message frames.

11. A device for controlling the transmission of messages between at least one wired network and at least one wireless network comprising:

a first interface means for coupling the device to the at least one wired network;

a second interface means for coupling the device to the at least one wireless network; and

a third interface means for interconnecting the first interface means and the second interface means, said third interface means including a filtering means for receiving messages from the at least one wired network correlating selected parameters in selected ones of the messages received to parameters stored in said device and forwarding messages to said at least one wireless network if the selected parameters in said selected ones of the messages correspond to selected ones of the parameters stored and forwarding to the at least one wireless network only those messages requiring action from a node on said at least one wireless network.

12. The communications network set forth in claim 10 wherein the additional parameters are a function of traffic on said communications network.

* * * * *

31/3,K/5 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015238378 **Image available**
WPI Acc No: 2003-299304/200329
Related WPI Acc No: 2005-283164
XRPX Acc No: N03-238083

Communication establishment method for cellular **communication system, involves receiving general and** specific **poll responses with same user ID from** mobile **station, for establishing communication with** base station

Patent Assignee: ANDERSON G B (ANDE-I); GAVETTE S (GAVE-I); JENSEN R N (JENS-I); PETCH B K (PETC-I); PETERSON P O (PETE-I); INTEL CORP (ITLC)
Inventor: ANDERSON G B; GAVETTE S; JENSEN R N; PETCH B K; PETERSON P O
Number of Countries: 001 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20020196840	A1	20021226	US 99307614	A	19990507	200329 B
			US 2002202756	A	20020725	
US 6947469	B2	20050920	US 99307614	A	19990507	200562
			US 2002202756	A	20020725	

Priority Applications (No Type Date): US 99307614 A 19990507; US 2002202756 A 20020725
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020196840	A1		18	H04B-001/69	Cont of application US 99307614
US 6947469	B2			H04B-001/69	Cont of application US 99307614

Communication establishment method for cellular **communication system, involves receiving general and** specific **poll responses with same user ID from** mobile **station, for establishing communication with** base station

Abstract (Basic):
... A general poll message with **base station** (BS) ID, is transmitted by BS (104) to **mobile** station (102) which in turn transmits response with user ID. The BS transmits **specific** poll message along with user ID to **mobile** station which transmits **specific** poll response only if message is received without error and with the same ID. The BS starts communicating with the **mobile** station, after receiving both the response messages.
... For **cellular** mobile telephone system, **preferably one** using a spread-spectrum technique, e.g. in the PCS band...

...a simple and flexible over-air protocol which supports an unlimited number of users and **base stations** . Minimizes interference between neighboring **base stations** . Protects communication against errors since user **ID verification** is repeatedly performed...

...The figure shows a network architecture illustrating connections between **base station** and network...

... **mobile** station (102...

... **base station** (104
...Title Terms: **CELLULAR** ;
Manual Codes (EPI/S-X): **W01-B05A1A** ...

... W01-B09 ...

... W02-C03C1A ...

... W02-C03C1G

US 20020196840A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2002/0196840 A1**

Anderson et al. (43) **Pub. Date: Dec. 26, 2002**

(54) **METHOD AND APPARATUS FOR WIRELESS SPREAD SPECTRUM COMMUNICATION WITH PREAMBLE PROCESSING PERIOD**

(76) Inventors: **Gary B. Anderson**, Carnelian Bay, CA (US); **Bryan K. Petch**, Colorado Springs, CO (US); **Peter O. Peterson**, Colorado Springs, CO (US); **Ryan N. Jensen**, Colorado Springs, CO (US); **Sherman Gavette**, Colorado Springs, CO (US)

Correspondence Address:
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD, SEVENTH FLOOR
LOS ANGELES, CA 90025 (US)

(21) Appl. No.: **10/202,756**

(22) Filed: **Jul. 25, 2002**

Related U.S. Application Data

(63) Continuation of application No. 09/307,614, filed on May 7, 1999.

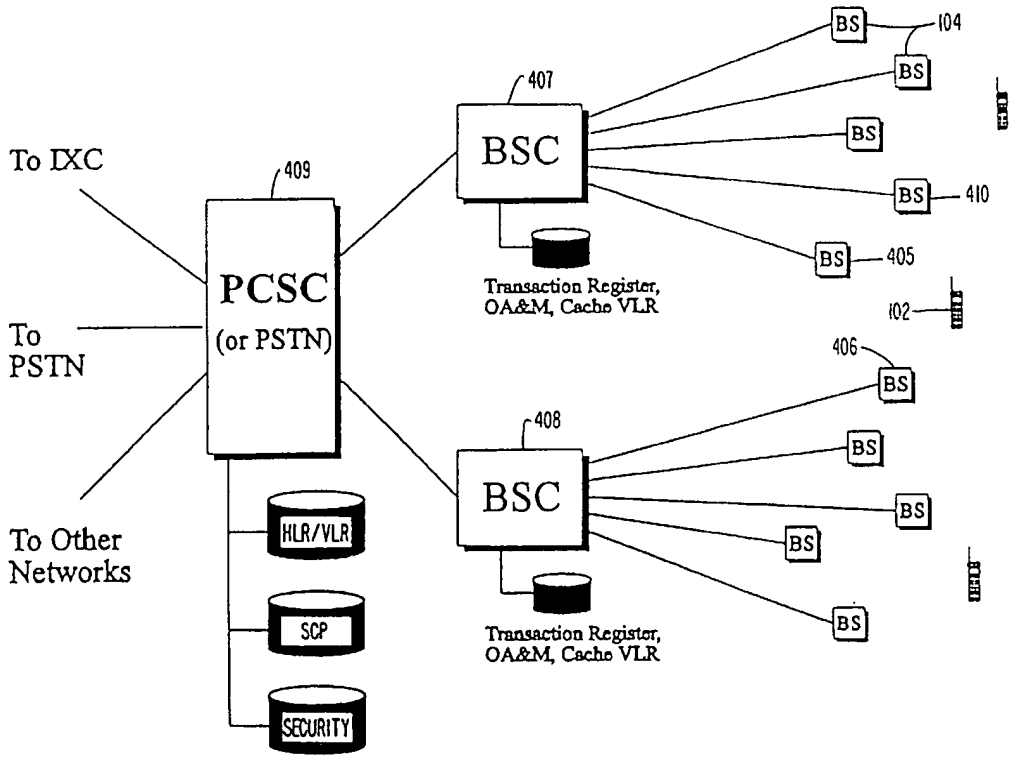
Publication Classification

(51) **Int. Cl.**[7] **H04B 1/69**

(52) **U.S. Cl.** **375/130**

(57) **ABSTRACT**

A simple and flexible over-air protocol for use with a mobile telephone system, having hand-held telephones in a micro-cell or other type of cellular communication system. A method in which user stations communicate with one or more base stations to place and receive telephone calls, in which the user stations are provided a secure voice or data link and have the ability to handoff calls between base stations while such calls are in progress. Each base station has a set of "air channels" to which it transmits in sequence. The air channels supported by each base station are called that base station's "polling loop". A user station receives general polling information on an unoccupied air channel, transmits responsive information to the base station, and awaits acknowledgment from the base station. Each base station may therefore simultaneously maintain communication with as many user stations as there are air channels in its polling loop. The ability of a user station to communicate on any unoccupied air channel makes the protocol air-channel agile, while the stability of user station and base station clocks may define air channels, gaps, and minor frames.



tion are interrupted. When a threshold for an error rate is exceeded, the base station **104** and user station **102** each independently stop sending data in information messages **303** and information responses **306**, and return to the specific poll step **310** for resynchronization. In an embodiment where the specific poll message has been eliminated as redundant, the base station **104** and the user station **102** may determine resynchronization by means of a designated bit in the header field **207**.

[0135] At the specific poll step **310**, the base station **104** transmits the specific poll message **302** and the user station **102** searches the major frame **201** for a specific poll message **302** having a user ID **309** which matches its own user ID **309**. After this handshaking succeeds, the base station **104** and user station **102** return to the link-established step **311** and continue transmitting and receiving information messages **303** and information responses **306**.

[0136] This technique for recovery from desynchronization, also called "reacquiring the base station," has the advantage that both the base station **104** and the user station **102** independently reverify the user ID **309** before communication is resumed. This assures that the base station **104** and the user station **102** stay in synchrony and communicate only on the agreed air channel **203**. Should the base station **104** and the user station **102** be unable to reestablish the communication link **312**, the telephone call will be terminated by the base station **104**.

[0137] At the link-established step **311**, the base station **104** also repeatedly and periodically transmits the user ID **309** in the D field **208** of the information message **303**. The user station **102** checks the user ID **309** to assure that the base station **104** and the user station **102** are each communicating on the proper air channel **203**. If this user ID **309** does not match, it returns to the specific poll step **310** to reacquire the base station **104**, as noted above.

[0138] Protocol Flexibility

[0139] The protocol described above provides flexibility with a small number of unique messages. The protocol is immune to changes in polling loop length and in the number of air channels allowed. The number of simultaneous users is therefore responsive to voice compression and data rate constraints and not by the protocol. The protocol also provides for an unlimited number of user stations in a given area, with the provision that the number of simultaneous calls cannot exceed the number of air channels. An unlimited number of base stations are also supported, making base station geography a function of available frequencies and range, not of protocol. The ability to interrogate and acquire alternate base stations in the presence of faulty communication provides for the expansion of a microcell network which may use base station handoff to route calls to base stations within range.

[0140] System Synchronization

[0141] In order to maximize system throughput capacity, the TDMA frame times for all base stations **104** within a geographical region are preferably synchronized to within a specified tolerance. For example, in one embodiment, all base stations **104** begin transmissions for the same frame within 6 microseconds.

[0142] The primary data timing standard in a digital network backhaul system, such as T1, ISDN BRI, or PRI, is the public switched telephone network (PSTN) timing standard. To prevent data precession into over run or under run, all base station controllers **105** and base stations **104** in such systems are synchronized to the PSTN timing standard.

[0143] At the system level, a GPS receiver is used at each base station controller **105** (and optionally at each base station **104**) to generate the primary reference timing marker for the TDMA frame timing. This marker is captured at the base station controller **105** every second and transmitted to the attached base stations **104**. A base station controller may temporarily turn off any major frame **201** or minor frame **202** of a given cell **103** which may be interfering with a neighboring cell **103**.

[0144] Each base station **104** provides the basic TDMA loop timing structure for its cell or sector. As previously noted, a synchronization preamble in the form a control pulse **215** or power control command is transmitted at the beginning of each minor frame **202** by the user station **102** and the base station **104**, respectively. When the appropriate preamble, consisting of a code sequence 48 chips in length, is received, a digital correlator (i.e., a matched filter) attuned to the specific preamble generates an internal synchronization pulse which may be very brief (e.g., two chips in duration, or 400 nanoseconds). The internal synchronization pulse may then be used to synchronize the start of M-ary symbol detection process.

[0145] Alternative Embodiments

[0146] While preferred embodiments are disclosed herein, many variations are possible which remain within the concept and scope of the invention, and these variations would become clear to one of ordinary skill in the art after perusal of the specification, drawings and claims herein.

[0147] For example, information which is transmitted from transmitter to receiver is referred to herein as "data", but it would be clear to those of ordinary skill in the art, after perusal of this application, that these data could comprise data, voice (encoded digitally or otherwise) error-correcting codes, control information, or other signals, and that this would be within the scope and spirit of the invention.

[0148] Moreover, while the specification has been described with reference to TDMA multiplexing of air channels, it would be clear to those of ordinary skill in the art, after perusal of this application, that air channels may be multiplexed by other means, including FDMA (frequency division multiplexing), by assigning air channels to differing frequency bands, CDMA (code division multiplexing), by assigning air channels to differing spread-spectrum spreading codes, other multiplexing techniques, or combinations of these multiplexing techniques, and that this would be within the scope and spirit of the invention.

What is claimed is:

1. In a communication system having a base station and a plurality of user stations, a method of establishing communication between said base station and one of said plurality of user stations, comprising the steps of

transmitting a general polling message from said base station;

receiving said general polling message at said one user station;

transmitting a general polling response from said user station;

receiving said general polling response at said base station;

transmitting a specific polling message from said base station;

receiving said specific polling message at said one user station;

transmitting a specific polling response from said one user station;

receiving said specific polling response at said base station; and

thereafter transmitting and receiving information messages between said base station and said one user station over an established communication link.

* * * * *

31/3,K/23 (Item 23 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012599184 **Image available**
WPI Acc No: 1999-405290/ **199934**
XRPX Acc No: N99-302115
Identifying **network layer** protocol **data unit**
Patent Assignee: NOKIA TELECOM OY (OYNO); NOKIA NETWORKS OY (OYNO)
Inventor: VIALEN J
Number of Countries: 084 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9933288	A1	19990701	WO 98FI991	A	19981217	199934	B
FI 9704560	A	19990619	FI 974560	A	19971218	199938	
AU 9916741	A	19990712	AU 9916741	A	19981217	199950	
FI 105985	B1	20001031	FI 974560	A	19971218	200058	
US 6831913	B1	20041214	WO 98FI991	A	19981217	200501	
			US 2000581913	A	20000721		

Priority Applications (No Type Date): FI 974560 A 19971218
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9933288	A1	E	26	H04Q-007/20	

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW

FI 9704560	A	H04Q-007/20	
AU 9916741	A	H04Q-007/20	Based on patent WO 9933288
FI 105985	B1	H04Q-007/20	Previous Publ. patent FI 9704560
US 6831913	B1	H04J-003/24	Based on patent WO 9933288

Identifying **network layer** protocol **data unit**

Abstract (Basic):
... A **cellular radio** network typically includes a network part and **mobile** stations (150) and the **base stations** (100) are controlled in a centralized manner by a **base station** controller. The **base stations** typically comprise 1-16 transceivers (114) offering **radio** capacity to 1 time division **multiple** access frequency, I.e. typically 8 time slots.
... The control unit (118) of the **base station** controls the operation of the transceivers and a multiplexer (116), arranging the traffic and control channels used in a **single** transmission connection (160), while an antenna unit (112) provides bi-directional **radio** connection to a **mobile** station **INDEPENDENT** CLAIMS are included for a **cellular radio** network and for a protocol data unit (PDU...

...Identifying a PDU in a network layer of air interface in **cellular radio** network...

...Reduced size of PDU by using unreserved value of protocol **discriminator**
.
...

...The drawing shows the the drawing illustrates an example of a **cellular radio** network structure...

... **Mobile** station (150...

... **Base station** (100
...International Patent Class (Main): **H04Q-007/20**
Manual Codes (EPI/S-X): **W01-A03A2** ...

... **W01-B05A1A** ...

... **W01-B05A1B** ...
... **W02-C03C1** ...

... **W02-C03C1B** ...

... **W02-C03C3**

US006831913B1

(12) **United States Patent**
Vialen

(10) **Patent No.: US 6,831,913 B1**
(45) **Date of Patent: Dec. 14, 2004**

(54) **METHOD OF IDENTIFYING NETWORK LAYER PDU**

(75) Inventor: **Jukka Vialen**, Espoo (FI)

(73) Assignee: **Nokia Networks Oy**, Espoo (FI)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/581,913**

(22) PCT Filed: **Dec. 17, 1998**

(86) PCT No.: **PCT/FI98/00991**

§ 371 (c)(1),
(2), (4) Date: **Jul. 21, 2000**

(87) PCT Pub. No.: **WO99/33288**

PCT Pub. Date: **Jul. 1, 1999**

(30) **Foreign Application Priority Data**

Dec. 18, 1997 (FI) 974560

(51) **Int. Cl.**[7] **H04J 3/24**
(52) **U.S. Cl.** **370/349**; 370/469
(58) **Field of Search** 370/328, 329, 370/330, 345, 348, 349, 466, 467, 469

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,563,879	A		10/1996	Sanders et al.
5,566,170	A		10/1996	Bakke et al.
5,841,764	A	*	11/1998	Roderique et al. 370/310
5,923,649	A	*	7/1999	Raith 370/328
5,956,646	A	*	9/1999	Kolev et al. 455/502
6,034,949	A	*	3/2000	Gellhaus et al. 370/252

FOREIGN PATENT DOCUMENTS

FR	2 724 278	3/1996
JP	0 704 450	3/1995

OTHER PUBLICATIONS

ETS 300 939 (Aug. 1997, 2nd ed.), "Digital Cellular Telecommunications System (Phase 2+); Mobile Radio Interface Signalling Layer 3; General Aspects (GMS 04.07 version 5.2.0)" section 11 "Messages."

* cited by examiner

Primary Examiner—Kwang Bin Yao
(74) *Attorney, Agent, or Firm*—Pillsbury Winthrop LLP

(57) **ABSTRACT**

The invention relates to a method of identifying a protocol data unit in a network layer of an air interface in a cellular radio network, to a cellular radio network and to a protocol data unit. A network layer usually includes connection management, mobility management and radio resources management sublayers. In the invention, the radio resources management sublayer is replaced by a radio network sublayer. A protocol data unit header includes a protocol discriminator. Some of the protocol discriminator values are allocated to the identification of protocol data units in the connection management sublayer and the mobility management sublayer. According tot the invention, at least one unreserved value of the protocol discriminator is used for identifying protocol data units in the radio network sublayer.

15 Claims, 6 Drawing Sheets

	8	7	6	5	4	3	2	1	
0	x	x	x	x	0	0	0	0	GSM - group call control
1	x	x	x	x	0	0	0	1	GSM - broadcast call control
2	x	x	x	x	0	0	1	0	GSM - PDSS1
3	x	x	x	x	0	0	1	1	GSM - call related SS messages
4	x	x	x	x	0	1	0	0	GSM - PDSS2
5	x	x	x	x	0	1	0	1	GSM - mobility management messages
6	x	x	x	x	0	1	1	0	GSM - radio resources management messages
7	x	x	x	x	0	1	1	1	UMTS 1
8	x	x	x	x	1	0	0	0	UMTS 2
9	x	x	x	x	1	0	0	1	GSM - SMS messages
10	x	x	x	x	1	0	1	0	UMTS 3
11	x	x	x	x	1	0	1	1	GSM - non-call related SS messages
12	x	x	x	x	1	1	0	0	UMTS 4
13	x	x	x	x	1	1	0	1	UMTS 5
14	x	x	x	x	1	1	1	0	GSM - reserved for PD extension
15	x	x	x	x	1	1	1	1	GSM - reserved for test procedures

plural number of radio bearer set-up procedures can take place simultaneously. A radio bearer control management entity RBC_MGT creates separate control entities RBC_0, . . . RBC_N for each set-up procedure., When a control entity has received from the network a first protocol data unit informing the radio bearer identifier BID (Bearer Identifier) that corresponds to the transaction identifier TI, the transaction identifier can be released, the transaction means TI/BID then transferring following protocol data units to the correct control entity.

The bearer identifier BID is placed into the non-imperative portion of the protocol data unit as a standard information element. The transaction identifier TI is coded into a half octet, bit **8** being a flagbit and bits **7**, **6** and **5** providing the actual transaction identifier. A flagbit **0** indicates that the bearer identifier BID has not received any value yet. A flagbit **1** indicates that the protocol data unit contains the bearer identifier BID. A value 000 of the actual transaction identifier means that the transaction identifier is not in use, The transaction identifier can take seven actual values: 001, 010, 011, 100, 101, 110, 111. This also sets a limit to the number of simultaneous radio bearer set-up procedures initiated by the mobile station **150**.

When necessary, the control entities and the RRC entity transfer the protocol data unit also to other sublayers of the network layer for processing.

An extra advantage provided by the described method is that introduction of new functions for processing by the radio network sublayer allows the radio network sublayer to read any messages it finds interesting as they pass through, although they are addressed to upper sublayers, and to take the information it needs. Messages of interest are identified in the identifying means PD on the basis of the protocol discriminator.

Another advantage is that messages of the upper sublayers (mobility management, control management) need not be conveyed over the air interface in the protocol data units of the radio network sublayer, but the radio network sublayer can directly check in the protocol discriminator which layer is to process the message concerned. A method of identification other than the one described in the invention would require the upper sublayer messages to be packed as data messages of the radio network sublayer before they are transferred over the air interface. This would introduce at least one additional octet to each message.

Processing by software, as described in connection with FIG. **6**, is carried out at the mobile station **150** also in the transmit direction, and in the base station system **126** in both transmit and receive direction.

Although the invention is described above with reference to an example shown in the accompanying drawings, it is apparent that the invention is not limited to it, but can vary in many ways within the inventive idea disclosed in the attached claims.

What is claimed is:

1. A method of identifying a protocol data unit in a network layer of an air interfaces in a cellular radio network, the network layer comprising a connection management sublayer and a mobility management sublayer, and the protocol data unit comprising a header which includes a protocol discriminator, some of the protocol discriminator values being allocated to the identification of protocol data units in the connection management sublayer and the mobility management sublayer, the method comprising:

using at least one unreserved value of the protocol discriminator for identifying protocol data units in a radio network sublayer.

2. The method according to claim **1**, wherein reserved values comprise the values 0, 1, 2, 3, 4, 5, 6, 9, 11, 14, 15.

3. The method according to claim **1**, wherein unreserved values comprise the values 7, 8, 10, 12, 13.

4. The method according to claim **1**, wherein the header comprises a transaction identifier which is used in a connection initiated by a mobile station.

5. The method according to claim **4**, wherein the transaction identifier is provided by a half octet unused by the protocol discriminator.

6. The method according to claim **1**, wherein the protocol data unit further comprises a radio bearer identifier.

7. The method according to claim **1**, wherein there is a one-to-one correspondence between the sublayers and the protocol data units.

8. A cellular radio network comprising:

a base station system,

a mobile station communicating with the base station system over an air interface, and

identifying means for identifying a protocol data unit in a network layer of the air interface by processing a protocol discriminator included in a header which the protocol data unit comprises, some of the protocol discriminator values of the identifying means being allocated to the identification of protocol data units in the connection management sublayer and the mobility management sublayer included in the network layer,

wherein the identifying means are arranged to use at least one unreserved value of the protocol discriminator for identifying protocol data units in a radio network sublayer.

9. The cellular radio network according to claim **8**, wherein reserved values of the identifying means comprise the values 0, 1, 2, 3, 4, 5, 6, 9, 11, 14, 15.

10. The cellular radio network according to claim **8**, wherein unreserved values of the identifying means comprise the values 7, 8, 10, 12, 13.

11. The cellular radio network according to claim **8**, further comprising transaction means for processing a transaction identifier included in the header, the transaction identifier being arranged to be used in a connection initiated by the mobile station.

12. The cellular radio network according to claim **11**, wherein the transaction means process an unused half octet of the protocol discriminator as the transaction identifier.

13. The cellular radio network according to claim **8**, further comprising transaction means for processing the radio bearer identifier included in the protocol data unit.

14. The cellular radio network according to claim **13**, wherein the transaction means are arranged to set a one-to-one correspondence between the sublayers and the protocol data units.

15. A protocol data unit in a network layer of an air interface in a cellular radio network, the network layer comprising a connection management sublayer and a mobility management sublayer, the protocol data unit comprising:

a header which includes a protocol discriminator, some of the protocol discriminator values being allocated to the identification of protocol data units in the connection management sublayer and the mobility management sublayer,

wherein at least one unreserved protocol discriminator value is allocated to the identification of protocol data units in the radio network sublayer.

* * * * *

31/3,K/19 (Item 19 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013120584 **Image available**
WPI Acc No: 2000-292455/200025
XRPX Acc No: N00-219346
Network-initiated change of mobile **phone parameters**
Patent Assignee: NOKIA MOBILE PHONES LTD (OYNO)
Inventor: SHAH B
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6047071	A	20000404	US 97837970	A	19970415	200025	B

Priority Applications (No Type Date): US 97837970 A 19970415
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6047071	A		9	H04L-009/00	

Network-initiated change of mobile **phone parameters**

Abstract (Basic):
... The method involves transmitting a call releasing message from a **base station** to a **mobile** phone after storing the updated operating parameters in a nonvolatile memory. The updated operating parameters corresponding to at least **one** parameter change code are downloaded from the **base station** to the **mobile** phone.
... An encrypting unit is used for securing communications between the **mobile** phones in a network. The **mobile** phone is programmed with a parameter change service **option** and at least **one** parameter change code for permitting over-the-air changing of operating parameters. A page message, which includes an inquiry as to the identity of the **mobile** phone and change service **option** , is transmitted from the **base station** within the network to the **mobile** phone. A page response message is transmitted from the **mobile** phone to the **base station** to **verify** the **identity** of the **mobile** phone and the presence of the parameter change service **option** . Instructions from the **base stations** are transmitted to the **mobile** phone to enter an over-the-air service providing process. At least **one** parameter change code from the **base station** is then transmitted to the **mobile** phone. The **mobile** phone transmits a response verifying at least **one** parameter change code. An **INDEPENDENT** CLAIM is also i ncluded for the **radio** communication network...

...Used in administration of parameters for operation of **mobile** telephones...
...Allows network-initiated over-the-air access to a **mobile** station's number **assignment** module (NAM) without requiring user intervention. Simplifies administration of NAM parameters by network service provider. Preserves security and integrity of NAM parameters to prevent unauthorized access. Maintains, changes and updates **mobile** phone parameters by a network service provider without requiring intervention by **mobile** phone user. Allows actions for protecting service provider's resources as well as to improve...

...deterrence and apprehension of persons who have hijacked a subscriber's account by stealing their **mobile** phone or by intercepting transmission from the **mobile** phone...
...Title Terms: **MOBILE** ;
International Patent Class (Main): **H04L-009/00**

Manual Codes (EPI/S-X): **W01-A05B** ...

... **W01-B05A1A** ...

... **W01-B05A1C** ...

... **W01-C02B6A** ...

... **W02-C03C1A**

US006047071A

United States Patent [19]

Shah

[11] Patent Number: 6,047,071

[45] Date of Patent: Apr. 4, 2000

[54] NETWORK-INITIATED CHANGE OF MOBILE PHONE PARAMETERS

[75] Inventor: **Bharat Shah**, San Diego, Calif.

[73] Assignee: **Nokia Mobile Phones**, Espoo, Finland

[21] Appl. No.: **08/837,970**

[22] Filed: **Apr. 15, 1997**

[51] **Int. Cl.**[7] **H04L 9/00**

[52] **U.S. Cl.** **380/273**; 380/271; 380/247; 380/248; 380/249; 455/410; 455/435; 455/551

[58] **Field of Search** 455/410, 411, 455/433, 435, 458, 551, 33.1; 380/247, 248, 249, 271, 273

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,993,067	2/1991	Leopold	380/21
5,077,790	12/1991	D'Amico et al.	380/23
5,146,498	9/1992	Smith	380/21
5,252,964	10/1993	Tan et al.	340/825.48
5,294,191	3/1994	Gerszberg	379/59
5,297,192	3/1994	Gerszberg	379/59
5,301,232	4/1994	Mulford	380/21
5,381,138	1/1995	Stair et al.	340/825.44
5,414,753	5/1995	Ehara	379/58
5,551,073	8/1996	Summarco	455/89
5,603,084	2/1997	Henry, Jr. et al.	455/33.1
5,722,084	2/1998	Chakrin et al.	455/551
5,790,952	8/1998	Seazholtz et al.	455/432
5,793,866	8/1998	Brown et al.	380/2
5,850,445	12/1998	Chan et al.	380/23
5,875,394	3/1999	Daly et al.	455/411
5,878,339	3/1999	Zicker et al.	455/419
5,898,783	4/1999	Rohrbach	380/49
5,918,177	6/1999	Corriveau et al.	455/432

OTHER PUBLICATIONS

"Network Initiated OTASP" by Semyon (Simon) Misikovsky, Dec. 4, 1996, Lucent Technologies.

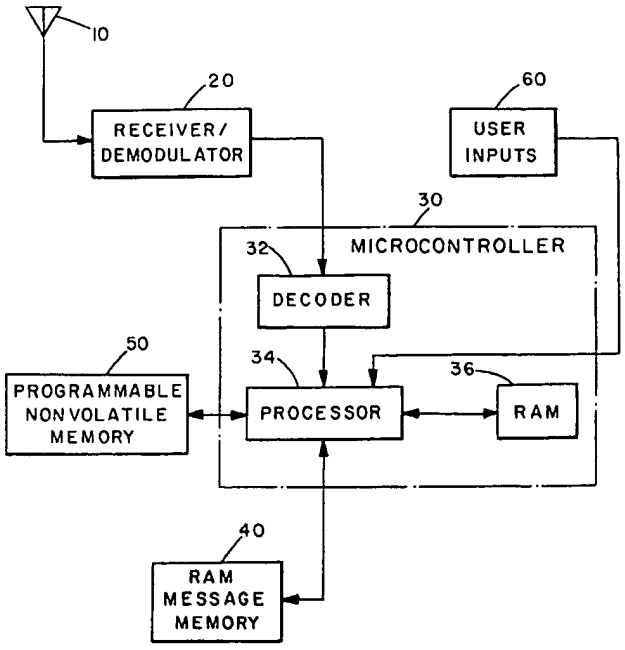
"Over–The–Air Parameter Administration Stage 1 description V1.03" Steve Thomas, Feb. 27, 1997, Telecommunications Industry Association.

Primary Examiner—Tod R. Swann
Assistant Examiner—Paul E. Callahan
Attorney, Agent, or Firm—Brown, Martin, Haller & McClain

[57] **ABSTRACT**

The procedure for Over-The-Air Parameter Administration (OTAPA) utilizes the over-the-air programming protocol and procedures which support the Over-The-Air Service Provisioning (OTASP) feature in accordance with established industry standards (TIA/EIA/IS-683). The mobile phone is programmed with a service option for changing the NAM parameters including an identification number for this option. The network base station sends a message to the mobile phone using the identification number and, if the mobile phone has OTAPA capability, it responds indicating support. The base station then transmits message telling the mobile station to proceed to the Traffic Channel and inquires whether the encryption mode is enabled, proceeding with the OTAPA only if the encryption mode is enabled. Once on the Traffic Channel, a Parameter Change Code (PCC) is sent. If the PCC is verified by the mobile unit, the base station proceeds to update the parameters and store the updated parameters into the phone's memory. After verification of the programmed data in accordance with OTASP processing, the process is terminated. No user intervention is required to initiate or conduct the OTAPA procedure.

30 Claims, 2 Drawing Sheets



In FIG. 2, the Mobile Station is generally designated as **100** and the Base Station as **200**. Mobile Station **100** is in the Idle State **101** when, at the direction of the Network Service Administrator, Base Station **200** initiates a Mobile terminated call **201** on Paging Channel **150**, sending a General Page Message **202** which includes the OTAPA service option (SERVICE_OPTION X set to "1"). Mobile Station **100** receives the page message and processes the OTAPA Service Option request **102**. Per the assumptions, Mobile Station **100** supports the OTAPA Service Option. Mobile Station **100** responds on Access Channel **160**, sending a Page Response Message **103** confirming the mobile's support of the OTAPA Service Option. Base Station **200** Process the Page Response Message and enables the Signaling Message Encryption (SME) **203** and, still on Paging Channel **150**, sends a Channel Assignment Message **204** which includes the encryption mode turned on (ENCRYPT_MODE set to "01"). Mobile Station **100** processes the Channel Assignment Message and verifies the SME, then sets up the designated Traffic Channel **170** according to IS-95 procedures **104**.

Base Station **200** sends a Data Burst Message using OTASP BURST-TYPE fields **205** and transmits the message to Mobile Station **100** over Traffic Channel **170**. This message includes a Protocol Capability Request Message. (All subsequent communications for this procedure occur over Traffic Channel **170**.) Mobile Station **100** processes Data Burst Message **205** and enters into the OTASP process according to IS-683 (step **105**), and responds to indicate OTAPA feature capability **105** by sending a Protocol Capability Response Message in step **106**. In step **206**, Base Station **200** transmits the Parameter Change Code (PCC) for the Mobile Station **100**. If the Mobile Station has more than one PCC, the Base Station **200** will specifically select the PCC for updating the Roaming List. Assuming the PCC is correct, Mobile Station **100** receives and validates the transmitted PCC.

Still communicating over Traffic Channel **170**, in steps **207** and **107**, Base Station **200** and Mobile Station **100**, respectively, follow the System Selection for Preferred Roaming (SSPR) procedure for Roaming List update as set forth in IS-683-A. After the updated roaming information is fully downloaded, in step **208**, Base Station **200** initiates the OTASP Data Commit process by sending a Data Commit Message (OTASP_MSG TYPE field set to "00000101") in accordance with IS-683, telling Mobile Station **100** to process and update the Roaming List. Mobile Station receives the Data Commit Message and sets the field of the data commit result code to indicate acceptance of the Data Commit Message (RESULT_CODE set to "00000000") and to store the new data in permanent memory. (Note that, in accordance with IS-683), if any errors are detected in the data, the RESULT_CODE will be set to the appropriate value to indicate the nature of the error.) After acceptance is indicated by Mobile Station **100**, the call is released.

The Over-The-Air Parameter Administration method of the present invention provide the advantage of allowing a network service provider to initiated over-the-air access to a mobile station's Number Assignment Module (NAM) without requiring user intervention, allowing for actions to be taken to protect the service provider's resources as well as to improve service to its subscribers. The strict enforcement of encryption procedures provides means for preserving security and integrity of NAM parameters to prevent unauthorized access, including unauthorized switching of service providers or "slamming". The inventive procedure also may be useful in assisting in the deterrence and apprehension of persons who have hijacked a subscriber's account by stealing their mobile phone or by intercepting and using a transmission from a mobile station. The OTAPA procedure can be initiated using existing OTASP protocols and procedures, requiring minimal changes to standards.

Other embodiments and modifications of the present invention will occur readily to those skilled in the art in view of these teachings. Therefore, this invention is to be limited only by the following claims, which include other embodiments and modifications when viewed in conjunction with the above specification and accompanying drawings.

I claim:

1. A method for making changes in at least one of a plurality of operating parameters of a mobile phone which operates within a network, the plurality of operating parameters being stored within a non-volatile memory, the method comprising:

providing an encryption means for securing communications between the mobile phone and the network;

programming the mobile phone with a parameter change service option and at least one parameter change code for permitting over-the-air changing of operating parameters;

transmitting a page message from a base station within the network to the mobile phone, the page message including an inquiry as to the identity of the mobile phone and the presence of the parameter change service option;

transmitting a page response message from the mobile phone to the base station verifying the identity of the mobile phone and the presence of the parameter change service option;

transmitting instructions from the base station to the mobile phone to enter an over-the-air service provisioning process;

transmitting the at least one parameter change code from the base station to the mobile phone;

transmitting from the mobile phone to the base station a response verifying the at least one parameter change code;

downloading updated operating parameters corresponding to the at least one parameter change code from the base station to the mobile phone;

storing the updated operating parameters in the non-volatile memory; and

transmitting from the base station to the mobile phone a call releasing message.

2. The method of claim **1**, wherein the encryption means comprises a programmable encryption mode and the step of programming the mobile phone includes programming the programmable encryption mode to enable message encryption.

3. The method of claim **2**, wherein the page message includes an inquiry to confirm that the programmable encryption mode is enabled.

4. The method of claim **1**, wherein the encryption means comprises a permanent encryption code for encrypting all communications between the mobile phone and the base station.

5. The method of claim **1**, wherein the plurality of operating parameters are divided into a plurality of parameter groups and wherein said at least one parameter change code comprises a plurality of parameter change codes with one parameter change code corresponding to each parameter group of the plurality of parameter groups.

6. The method of claim **1**, wherein the at least one parameter change code is an authentication key for the mobile phone.

7. The method of claim 1, wherein the step of determining whether the mobile phone is set up for message encryption comprises:

transmitting a channel assignment message from the base station to the mobile phone wherein the channel assignment message has an encryption mode turned on; and

transmitting a response from the mobile phone to the base station verifying that the encryption mode is turned on.

8. The method of claim 1, wherein the step of programming the mobile phone comprises assigning one service option number from a plurality of service option numbers for the parameter service option and setting the value of the one service option number to "1".

9. The method of claim 8, wherein the page response message includes a field containing the one service option number.

10. The method of claim 1, wherein the at least one parameter change code has a pre-set value.

11. The method of claim 10, wherein the pre-set value of the at least one parameter change code may be changed to a different value only by intervention of a user of the mobile phone.

12. The method of claim 1, wherein the step of downloading updated operating parameters includes downloading the updated operating parameters using the over-the-air service provisioning process according to the IS-683 standard.

13. A method of claim 1, wherein the step of determining whether the mobile phone is set up for message encryption further includes transmitting a channel assignment message to the mobile phone.

14. The method of claim 1, wherein the step of transmitting instructions to enter an over-the-air service provisioning process includes transmitting data burst messages.

15. A wireless communications network having a base station with a service administrator, and a mobile station, the mobile station having a plurality of operating parameters stored within a non-volatile memory, at least a portion of the plurality of operating parameters which may be changed by the service administrator, the network comprising:

message encryption means for securing communications between the base station and the mobile station;

means for programming the memory of the mobile station wherein the mobile station has programmable options for over-the-air parameter changes, the mobile station being set to enable the programmable options;

means for initiating a call from the base station to the mobile station when the mobile station is in an idle mode, the call comprising a paging message for interrogating the mobile station to confirm a mobile station identity and that the programmable options for over-the-air parameter changes are enabled;

means for terminating the call if the programmable options for over-the-air parameter changes are not enabled;

means for instructing the mobile phone to enter into an over-the-air service provisioning process;

means for enabling a download of updated operating parameters from the base station to the mobile station including transmitting a parameter change code portion within the programmable options for over-the-air parameter changes;

means for storing the updated operating parameters in the non-volatile memory; and

means for terminating the call.

16. The network of claim 15, wherein the message encryption means comprises a programmable encryption mode and the means for programming the memory of the mobile station includes means for programming the programmable encryption mode to enable message encryption.

17. The network of claim 16, wherein the paging message includes an inquiry to confirm that the programmable encryption mode is enabled.

18. The network of claim 15, wherein the message encryption means includes a permanent encryption code for encrypting all communications between the mobile station and the base station.

19. The network of claim 15, wherein the over-the-air service provisioning process is in accordance with the IS-683 standard.

20. The network of claim 15, wherein the plurality of operating parameters are divided into a plurality of parameter groups and each parameter group of the plurality has a corresponding parameter change code.

21. The network of claim 15, wherein the parameter change code is an Authentication key for changing a Shared Secret Data set of the mobile station.

22. The network of claim 15, wherein the paging message includes a channel assignment message from the base station to the mobile phone wherein the channel assignment message has an encryption mode turned on and a response message from the mobile phone to the base station verifying that the encryption mode is turned on.

23. The network of claim 15, wherein the means for programming includes a data field having a plurality of service option numbers including one service option number corresponding to a parameter service option for over-the-air parameter changes and setting the value of the one service option number to "1".

24. The network of claim 15, wherein the parameter change code portion has a pre-set value.

25. The network of claim 24, wherein the pre-set value of the parameter change code portion may be changed to a different value only by intervention of a user of the mobile station.

26. A method for administering a wireless communications network comprising a base station and a plurality of mobile phones, each mobile phone having an identity and a plurality of operating parameters stored in a non-volatile memory, at least a portion of the operating parameters which require updating, wherein a user of the mobile phone is not required to initiate a procedure for updating the operating parameters, the method comprising:

programming the mobile phone with a parameter change service option and at least one parameter change code for permitting over-the-air changing of operating parameters;

when an update to the operating parameters is required, transmitting a General Page Message from a base station to the mobile phone in an Idle Mode, the General Page Message including a request to verify the identity of the mobile phone and a first data field for the parameter change service option;

receiving a Page Response Message from the mobile phone to the base station including the identity of the mobile phone and the first data field for the parameter change service option;

transmitting a Channel Assignment Message from the base station to the mobile phone, the Channel Assignment Message including a second data field for message encryption and instructing the mobile phone to set up a traffic channel;

receiving a response from the mobile phone including the second data field to verify message encryption;

terminating the transmission from the base station if message encryption is not verified;

transmitting a Data Burst Message from the base station to the mobile phone instructing the mobile phone to enter an over-the-air service provisioning process;

transmitting a Protocol Capability Request Message from the base station to the mobile phone, the Protocol Capability Request Message including a third data field for feature capability of the mobile phone;

receiving a Protocol Capability Response Message from the mobile phone indicating the third data field;

transmitting the at least one parameter change code from the base station to the mobile phone;

transmitting from the mobile phone to the base station a response verifying the at least one parameter change code;

downloading updated operating parameters corresponding to the at least one parameter change code from the base station to the mobile phone; and

transmitting a Data Commit Message from the base station to the mobile phone for storing the updated operating parameters in the non-volatile memory and for releasing the call.

27. The method of claim **26**, wherein the at least one parameter change code has a pre-set value.

28. The method of claim **27**, wherein the pre-set value of the at least one parameter change code may be changed to a different value only by intervention of a user of the mobile phone.

29. The method of claim **26**, wherein the step of downloading updated operating parameters includes downloading the updated operating parameters using the over-the-air service provisioning process according to the IS-683 standard.

30. The method of claim **26**, wherein the at least one parameter change code is an A-key for changing a set of Shared Secret Data for the mobile phone.

* * * * *

31/3,K/16 (Item 16 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013432033 **Image available**
WPI Acc No: 2000-603976/200058
XRPX Acc No: N00-447029

Lightweight Internet protocol encapsulated scheme for multimedia traffic transported in a packet communication system

Patent Assignee: LUCENT TECHNOLOGIES INC (LUCE)
Inventor: CHUAH M; FLEISCHER W; YAN A; YUE O; CHUAH M C
Number of Countries: 029 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1045562	A2	20001018	EP 2000301583	A	20000228	200058	B
CA 2299141	A1	20000908	CA 2299141	A	20000223	200060	
JP 2000286894	A	20001013	JP 200064098	A	20000308	200101	
KR 2000062759	A	20001025	KR 200010988	A	20000306	200124	
US 6993021	B1	20060131	US 99264053	A	19990308	200610	

Priority Applications (No Type Date): US 99264053 A 19990308
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1045562	A2	E	9	H04L-029/06	
	Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI				
CA 2299141	A1	E		H04L-012/56	
JP 2000286894	A		10	H04L-012/56	
KR 2000062759	A			H04L-012/56	
US 6993021	B1			H04L-012/56	

Abstract (Basic):
... A **base station** (1) receives voice traffic from **mobile** stations (10) and **multiplexes** the voice traffic from various sources into lightweight Internet protocol encapsulated (LIPE) packets, which are further encapsulated into user **identifier** /Internet **protocol** packets with a **multiplexing** header field including a 16 bit user identifier field, an 11 bit length indicator field, a 1 bit more field and an **optional** 8 bit payload type/class of service field. The length indicator field allows a maximum...

...of 2048 bytes and incoming data packets can be partitioned into multiple data packets. The **optional** payload field is partitioned into 3 bit fields used to identify the payload type.
... AN **INDEPENDENT** CLAIM is included for a method for use in a packet server...
...Packet communication between a **mobile** switching center and **base stations** .
...

...The drawing shows a portion of a **mobile** communication system embodying the invention...

... **Base station** (1...

... **Mobile** stations (10

International Patent Class (Main): **H04L-012/56** ...

... **H04L-029/06**
International Patent Class (Additional): **H04L-012/28**

Manual Codes (EPI/S-X): **W01-A03B** ...

... **W01-A06E1** ...

... **W01-A06F** ...

... **W01-A06G2** ...
... **W01-B05A1A** ...

... **W02-C03C1A**

US006993021B1

(12) **United States Patent**
Chuah et al.

(10) **Patent No.: US 6,993,021 B1**
(45) **Date of Patent: Jan. 31, 2006**

(54) **LIGHTWEIGHT INTERNET PROTOCOL ENCAPSULATION (LIPE) SCHEME FOR MULTIMEDIA TRAFFIC TRANSPORT**

(75) Inventors: **Mooi Choo Chuah**, Eatontown, NJ (US); **Wolfgang Fleischer**, Swindon (GB); **Anlu Yan**, Eatontown, NJ (US); **On-Ching Yue**, Middletown, NJ (US)

(73) Assignee: **Lucent Technologies Inc.**, Murray Hill, NJ (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/264,053**

(22) Filed: **Mar. 8, 1999**

(51) **Int. Cl.**
H04L 12/56 (2006.01)

(52) **U.S. Cl.** **370/389**; 370/466; 370/469

(58) **Field of Classification Search** 370/466, 370/467, 468, 469, 472, 473, 474, 476, 392–394
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,435,173	A		3/1984	Siposs et al. 604/155
4,457,751	A		7/1984	Rodler 604/66
5,065,398	A	*	11/1991	Takashima 370/230
5,594,732	A	*	1/1997	Bell et al. 370/401
5,713,856	A		2/1998	Eggers et al. 604/65
5,717,690	A	*	2/1998	Peirce et al. 370/389
5,734,653	A	*	3/1998	Hiraiwa et al. 370/395
5,931,961	A	*	8/1999	Ranganathan et al. 714/712
6,041,054	A	*	3/2000	Westberg 370/389
6,044,081	A	*	3/2000	Bell et al. 370/401
6,052,819	A	*	4/2000	Barker et al. 714/776
6,075,787	A	*	6/2000	Bobeck et al. 370/395
6,081,524	A	*	6/2000	Chase et al. 370/389
6,107,911	A		8/2000	Perrone 340/309.16
6,115,422	A	*	9/2000	Anderson et al. 375/240
6,122,670	A	*	9/2000	Bennett et al. 709/236
6,157,719	A	*	12/2000	Wasilewski et al. 380/21
6,160,793	A	*	12/2000	Ghani et al. 370/236
6,175,573	B1	*	1/2001	Togo et al. 370/474
6,205,148	B1	*	3/2001	Takahashi et al. 370/401
6,212,190	B1	*	4/2001	Mulligan 370/400
6,229,821	B1	*	5/2001	Bharucha et al. 370/471
6,229,823	B1	*	5/2001	Scarmalis 370/477
6,286,052	B1	*	9/2001	McCloghrie et al. 709/238
6,292,495	B1	*	9/2001	Von Hammerstein et al. 370/465
6,295,296	B1	*	9/2001	Tappan 370/392
6,330,242	B1	*	12/2001	Ogawa et al. 370/395.52
6,341,129	B1	*	1/2002	Schroeder et al. 370/354
6,366,961	B1	*	4/2002	Subbiah et al. 709/238
6,554,798	B1		4/2003	Mann et al. 604/131

(Continued)

FOREIGN PATENT DOCUMENTS

CA	2220252	9/1997

OTHER PUBLICATIONS

J. Rosenberg, "An RTP Payload Format for user Multiplexing", work in progress, draft-ietf-avt-aggregation-00.txt.

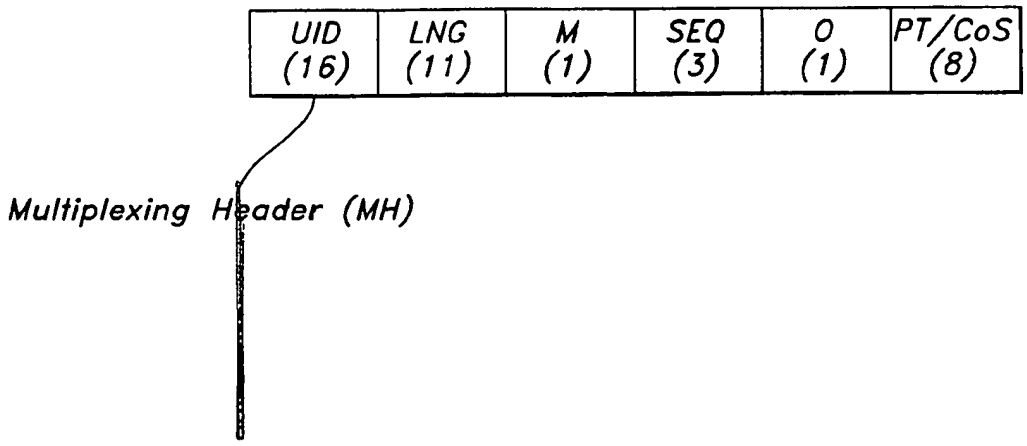
(Continued)

Primary Examiner—Chi Pham
Assistant Examiner—Thai Hoang

(57) **ABSTRACT**

A packet encapsulation scheme for multiplexing application sessions—Lightweight IP Encapsulation (LIPE)—is described. An LIPE packet comprises at least one multiplexing header (NH) and associated multimedia data packet (MDP). The LIPE packet uses UDP/IP as transport. An MH field further comprises a 16-bit a user identifier (UID) field, an 11 bit length indicator (LNG) field, a 1 bit "more" (M) field and an optional payload type/class of service (PT/CoS) field comprising 8 bits.

19 Claims, 8 Drawing Sheets



heterogeneous voice source types, while the CoS field gives the application the flexibility to choose different type of services, such as low loss or low delay, after the LIPE demultiplexing point.

The foregoing merely illustrates the principles of the invention and it will thus be appreciated that those skilled in the art will be able to devise numerous alternative arrangements which, although not explicitly described herein, embody the principles of the invention and are within its spirit and scope. For example, although the inventive concept was illustrated herein as being implemented with discrete functional building blocks, e.g., an LIPE formatter, etc., the functions of any one or more of those building blocks can be carried out using one or more appropriately programmed processors, e.g., a digital signal processor; discrete circuit elements; integrated circuits; etc. Further, although illustrated in the context of CDMA, the inventive concept is applicable to any wireless system (e.g., UMTS, etc.) or application that requires real-time multiplexing of data streams.

What is claimed is:

1. A method for use in a packet server, the method comprising the steps of:

receiving a number of incoming data packets;

formatting a multiplexing header for each incoming data packet, wherein the formatted multiplexing header includes a user identifier field, a length indicator field, a more packets field, a class of service field, and a sequence number field; and

multiplexing the formatted multiplexing headers and their associated incoming data packets into a single transport session.

2. The method of claim 1 wherein the formatting step encapsulates LIPE packets using Internet Protocol/User Datagram Protocol (IP/UDP) transport.

3. The method of claim 2 wherein the format for an encapsulated LIPE packet using (IP/UDP) transport comprises an IP header field, a UDP header field and at least one multiplexing header and an associated multimedia data packet, wherein the multiplexing header comprises a user identifier field, a length identifier field, and a more packets field, the more field being used to indicate the use of more than one multiplexing header and associated multimedia data packet for transporting incoming data packets.

4. The method of claim 1 wherein the more packets field is used to indicate the use of more than one multiplexing header and an associated data packet for transporting incoming data packets.

5. The method of claim 1 wherein the class of service field further comprises a number of bits representative of a payload type and a remaining number of bits representative of a quality of service.

6. The method of claim 5 wherein the number of bits representative of the payload type represent different voice coding schemes.

7. The method of claim 1, wherein, the number of incoming data packets is from a plurality of users.

8. A method for use in a packet server, the method comprising the steps of:

receiving a number of incoming data streams from a plurality of users;

formatting the incoming data packets into user datagram (UDP)/Internet Protocol (IP) packets such that each UDP/IP packet encapsulates at least a UDP header, an IP header and a formatted multiplexing header, wherein the formatted multiplexing header portion includes information for identifying an application associated with the payload, a user identifier field, a length indicator field, a more packets field, and a class of service field, where the more packets field is used to indicate the association of more than one data packet for the application.

9. The method of claim 8 wherein the class of service field further comprises a number of bits representative of a payload type and a remaining number of bits representative of a quality of service.

10. The method of claim 9 wherein the number of bits representative of the payload type represent different voice coding schemes.

11. A method for use in a packet server, the method comprising the steps of:

receiving a number of incoming LIPE packets associated with at least one of different applications and a plurality of users; and

formatting each of the incoming LIPE packets into user datagram (UDP)/Internet Protocol (IP) packets such that each UDP/IP packet encapsulates at least a UDP header, an IP header, a formatted multiplexing header and a payload portion, wherein the formatted multiplexing header portion includes information for identifying the different applications, a user identifier field, a length indicator field, a more packets field, and a class of service field, where the more packets field is used to indicate the association of more than one data packet for an application.

12. The method of claim 11 wherein the class of service field further comprises a number of bits representative of a payload type and a remaining number of bits representative of a quality of service.

13. The method of claim 12 wherein the number of bits representative of the payload type represent different voice coding schemes.

14. An improved apparatus for transporting packets, the improved apparatus comprising:

a reception unit adapted to receive a number of incoming data packets;

an analysis unit adapted to analyze multiplexing header information associated with each incoming data packet;

a formatting unit adapted to format a multiplexing header for each incoming data packet utilizing the analyzed multiplexing header information;

wherein the formatted multiplexing header includes a user identifier field, and length indicator field, a more packets field, a class of service field and a sequence number field, wherein the more packets field is used to indicate the use of more than one multiplexing header and associated data packet for transporting incoming data packets; and

a modulator unit adapted to multiplex the incoming data packets into a single transport session.

15. The improved apparatus of claim 14 wherein the formatting unit further encapsulates the incoming data packets using User Datagram Protocol/Internet Protocol (UDP/IP) transport.

16. The improved apparatus of claim 15 wherein the format for an encapsulated LIPE packet using (IP/UDP) transport comprises an IP header field, a UDP header field and at least one multiplexing header and an associated

multimedia data packet, wherein the multiplexing header comprises the user identifier field, length indicator field, and more packets field.

17. The improved apparatus of claim 14 wherein the class of service field further comprises a number of bits representative of a payload type and a remaining number of bits representative of a quality of service.

18. The improved apparatus of claim 17 wherein the number of bits representative of the payload type represent different voice coding schemes.

19. The method of claim 14 wherein the number of incoming data packets is from a plurality of users.

* * * * *

31/3,K/9 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014118462 **Image available**
WPI Acc No: 2001-602674/200168
Related WPI Acc No: 2002-643817
XRPX Acc No: N01-449725

Apparatus for mapping an Internet protocol address to a mobile **station integrated services digital network number in a** wireless **application processing network using a start packet from a server**

Patent Assignee: TELEFONAKTIEBOLAGET ERICSSON L M (TELF); BERG I (BERG-I) ; SKOG R (SKOG-I)
Inventor: BERG I; SKOG R
Number of Countries: 094 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200167716	A1	20010913	WO 2001SE409	A	20010223	200168 B
US 20010028636	A1	20011011	US 2000188437	P	20000310	200168
			US 2000596802	A	20000619	
			US 2001802521	A	20010309	
AU 200137852	A	20010917	AU 200137852	A	20010223	200204
US 6775262	B1	20040810	US 2000188437	P	20000310	200453
			US 2000596802	A	20000619	
US 20040260816	A1	20041223	US 2000188437	P	20000310	200504
			US 2000596802	A	20000619	
			US 2004891641	A	20040715	

Priority Applications (No Type Date): US 2000596802 A 20000619; US 2000188437 P 20000310; US 2001802521 A 20010309; US 2004891641 A 20040715
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200167716	A1	E	18	H04L-029/12	
					Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
					Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW
US 20010028636	A1			H04Q-007/00	Provisional application US 2000188437
					CIP of application US 2000596802
AU 200137852	A			H04L-029/12	Based on patent WO 200167716
US 6775262	B1			H04J-003/24	Provisional application US 2000188437
US 20040260816	A1			G06F-015/16	Provisional application US 2000188437
					Cont of application US 2000596802
					Cont of patent US 6775262

Apparatus for mapping an Internet protocol address to a mobile **station integrated services digital network number in a** wireless **application processing network using a start packet from a server**

Abstract (Basic):
... A remote authentication dial-in user service (**RADIUS**) server (60) is configured to transmit **radius** accounting messages from a **mobile** switching center/visitor location register (50) to a **wireless** application protocol (**WAP**) **gateway** (70) through **routers** (65) and an accounting server (75) is responsive to the message and updates the mapping session database (80) in the **gateway** . The database includes storage locations for an **assigned** temporary Internet protocol address

and an associated number of a **mobile** terminal (45). Information in a packet is used to update the database once a connection...

... **INDEPENDENT** CLAIMS are included for a method of associating a **mobile** station integrated services digital network (MSISDN) number with a temporary Internet protocol (IP) address...

...Mapping an IP address to a MSISDN number in a **WAP** processing network ...

... **RADIUS** server (60...

... **WAP** **gateway** (70...

... **Routers** (65...

... **Mobile** terminal (45

...Abstract (Equivalent): NOVELTY - A remote authentication dial-in user service (**RADIUS**) server (60) is configured to transmit **radius** accounting messages from a **mobile** switching center/visitor location register (50) to a **wireless** application protocol (**WAP**) **gateway** (70) through **routers** (65) and an accounting server (75) is responsive to the message and updates the mapping session database (80) in the **gateway** . The database includes storage locations for an **assigned** temporary Internet protocol address and an associated number of a **mobile** terminal (45). Information in a packet is used to update the database once a connection...

...DETAILED DESCRIPTION - **INDEPENDENT** CLAIMS are included for a method of associating a **mobile** station integrated services digital network (MSISDN) number with a temporary Internet protocol (IP) address...

...USE - Mapping an IP address to a MSISDN number in a **WAP** processing network...

... **RADIUS** server 60...

... **WAP** **gateway** 70...

... **Routers** 65...

... **Mobile** terminal 45

...Title Terms: **MOBILE** ;

International Patent Class (Main): **G06F-015/16** ...

... **H04L-029/12** ...

... **H04Q-007/00**

International Patent Class (Additional): **H04L-012/28** ...

... **H04L-012/56** ...

... **H04L-029/06**

Manual Codes (EPI/S-X): **W01-A06B7** ...

... **W01-B05A1A** ...

... **W01-C05B7** ...

... **W02-C03C1A**

US006775262B1

(12) **United States Patent**
Skog et al.

(10) **Patent No.: US 6,775,262 B1**
(45) **Date of Patent: Aug. 10, 2004**

(54) **METHOD AND APPARATUS FOR MAPPING AN IP ADDRESS TO AN MSISDN NUMBER WITHIN A WIRELESS APPLICATION PROCESSING NETWORK**

(75) Inventors: **Robert Skog**, Hasselby (SE); **Ingvar Berg**, Nykill (SE)

(73) Assignee: **Telefonaktiebolaget LM Ericsson (publ)**, Stockholm (SE)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 715 days.

(21) Appl. No.: **09/596,802**

(22) Filed: **Jun. 19, 2000**

Related U.S. Application Data

(60) Provisional application No. 60/188,437, filed on Mar. 10, 2000.

(51) **Int. Cl.**[7] **H04J 3/24**

(52) **U.S. Cl.** **370/349**; 370/389; 370/352; 370/401

(58) **Field of Search** 370/349, 345, 370/389, 467, 352, 465, 466, 338, 401, 354, 328; 455/433, 556, 426, 466, 435, 445; 709/206, 219; 705/44, 34

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,974,453 A	*	10/1999	Andersen et al.	709/220
6,516,197 B2	*	2/2003	Havinis et al.	455/456.1
6,549,776 B1	*	4/2003	Joong	455/433
6,608,832 B2	*	8/2003	Forslow	370/353
2002/0049675 A1	*	4/2002	Kailamaki et al.	705/44

FOREIGN PATENT DOCUMENTS

WO	WO 99/33291		7/1999	
WO	WO 00/04679	*	1/2000	H04L/12/28
WO	WO 00/46963	*	8/2000	H04L/12/66

OTHER PUBLICATIONS

Standard Search Report for RS 105432US Completed Jan. 19, 2001, Jan. 23, 2001, EPX.

M. Hoogenboom and P. Steemers, "Security for Remote Access and Mobile Applications", *Computers & Security, International Journal Devoted to the Study of Technical and Financial Aspects of Computer Security*, Elsevier Science Ltd., vol. 19, No. 2, Feb. 2000, pp. 149–163, XP004204675.

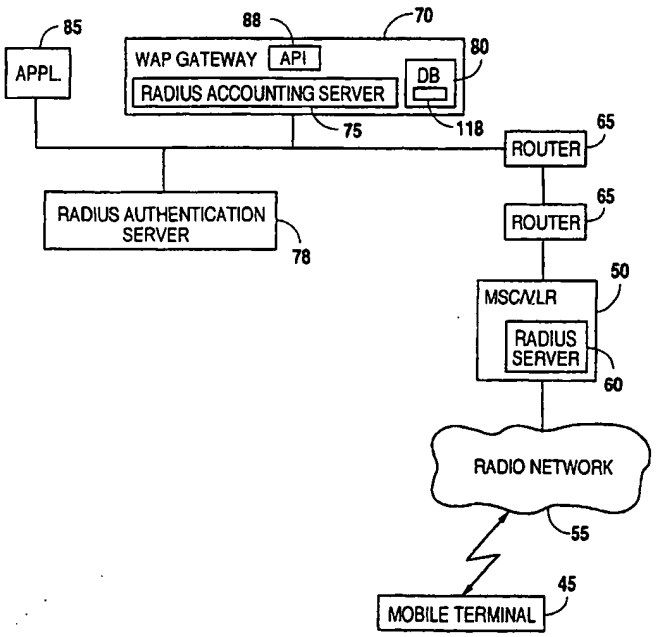
* cited by examiner

Primary Examiner—Wellington Chin
Assistant Examiner—Jamal A. Fox

(57) **ABSTRACT**

A system and method for associating an MSISDN of a mobile terminal with a temporarily assigned IP address is disclosed. A first server located within a wireless communications network generates and transmits a start packet to a WAP network responsive to an access request by a mobile terminal. The start packet includes the MSISDN of the mobile terminal and an assigned IP address. A second server within the WAP network extracts the MSISDN in the IP address from the received start packet and stores this information together within a database. When a WAP application is utilized, the MSISDN may be determined from the database and placed in an HTTP-header of packets to the WAP application.

12 Claims, 2 Drawing Sheets



Referring now to FIG. **4**, there is illustrated a signaling diagram wherein a mobile terminal **45** with an established PPP connection to the access server **60** terminates the PPP connection. Initially, the mobile station **45** terminates at **135** the PPP connection with the access server **60**. In response to the termination of the PPP connection, the access server **60** transmits an accounting request stop message **140** to the WAP gateway **70**. This request includes the MSISDN and IP address of the mobile terminal **45**. In response to the accounting request stop message **140**, the WAP gateway **70** removes the entry within the mapping session database **80** associated with the MSISDN number and IP address. The WAP gateway **70** responds to the accounting request stop message by means of an accounting response message **145** acknowledging cancellation of the PPP connection.

The previous description is of a preferred embodiment for implementing the invention, and the scope of the invention should not necessarily be limited by this description. The scope of the present invention is instead defined by the following claims.

What is claimed is:

1. A method for associating a MSISDN with a temporary IP address within a WAP network, comprising the steps of:

transmitting a start packet to a server associated with the WAP gateway node, the start packet including a MSISDN and a temporary IP address of the mobile terminal; and

storing the MSISDN and the temporary IP address in a database wherein the MSISDN and the temporary IP address are associated with each other responsive to the start packet,

when a WAP application is utilized, determining the MSISDN of the mobile terminal by accessing the database,

placing the determined MSISDN into an http header; and

transmitting the http header to a WAP application with a data packet,

configuring a RADIUS authentication server to transmit an account stop packet as the stop packet,

transmitting a stop packet to the server associated with the WAP gateway node, the stop packet including the MSISDN and the temporary IP address of the mobile terminal; and

deleting the stored MSISDN and the temporary IP address from the database responsive to the stop packet.

2. The method of claim **1**, further comprising the step of transmitting an acknowledgment packet from the server responsive to the stop packet.

3. The method of claim **1**, wherein the step of transmitting further comprises the step of configuring an access server to transmit starting packet as the start packet.

4. The method of claim **1**, wherein the step of transmitting further comprises the step of configuring the RADIUS authentication server to transmit an account starting packet as the start packet.

5. The method of claim **4**, further comprising the step of transmitting an acknowledgment packet from the server responsive to the start packet.

6. The method of claim **1**, wherein the method is used in at least one of an authentication process, a billing process, and a personalization process.

7. A system for associating a MSISDN of a mobile terminal with a temporarily assigned IP address, comprising:

a first server associated with a wireless network for generating a start packet responsive to an access request from a mobile terminal, the start packet containing a MSISDN provided by the mobile terminal and an IP address assigned to the mobile terminal by the first server.

a database associated with a WAP network having storage locations for a plurality of MSISDNs and associated assigned IP addresses; and

a second server associated with the WAP network for extracting the MSISDN and the IP address from the start packet and storing the MSISDN and the IP address in the database wherein the second server comprises a RADIUS accounting server including a translation application program interface for enabling access to the database by a WAP application configured to place the determined MSISDN into an http header; and transmit the http header to a WAP application with a data pack.

8. The system of claim **7**, wherein the second server is located within a WAP gateway of the WAP network.

9. The system of claim **7**, wherein the first server comprises an integrated access system server.

10. The system of claim **7**, wherein the second server is configured to:

receive the session start packet from the first server in response to an access request from the mobile terminal;

store the MSISDN number and the temporary IP-address in the database associated with the WAP gateway; and

update the mapping session database by removing the MSISDN number and the temporary IP-address in response to a receipt of a stop packet.

11. The system of claim **7**, wherein the first server further generates a stop packet responsive to termination of a connection with the mobile terminal.

12. The system of claim **7**, wherein the system associates a MSISDN of a mobile terminal with a temporarily assigned IP address during at least one of an authentication process, a billing process and a personalization process.

* * * * *

US 20040260816A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2004/0260816 A1**

Skog et al. (43) **Pub. Date: Dec. 23, 2004**

(54) **METHOD AND APPARATUS FOR MAPPING AN IP ADDRESS TO AN MSISDN NUMBER WITHIN A WIRELESS APPLICATION PROCESSING NETWORK**

(75) Inventors: **Robert Skog**, Hasselby (SE); **Ingvar Berg**, Nykil (SE)

Correspondence Address:
ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR C11
PLANO, TX 75024 (US)

(73) Assignee: **Telefonaktiebolaget LM Ericsson (publ)**, Stockholm (SE)

(21) Appl. No.: **10/891,641**

(22) Filed: **Jul. 15, 2004**

Related U.S. Application Data

(63) Continuation of application No. 09/596,802, filed on Jun. 19, 2000, now Pat. No. 6,775,262.

(60) Provisional application No. 60/188,437, filed on Mar. 10, 2000.

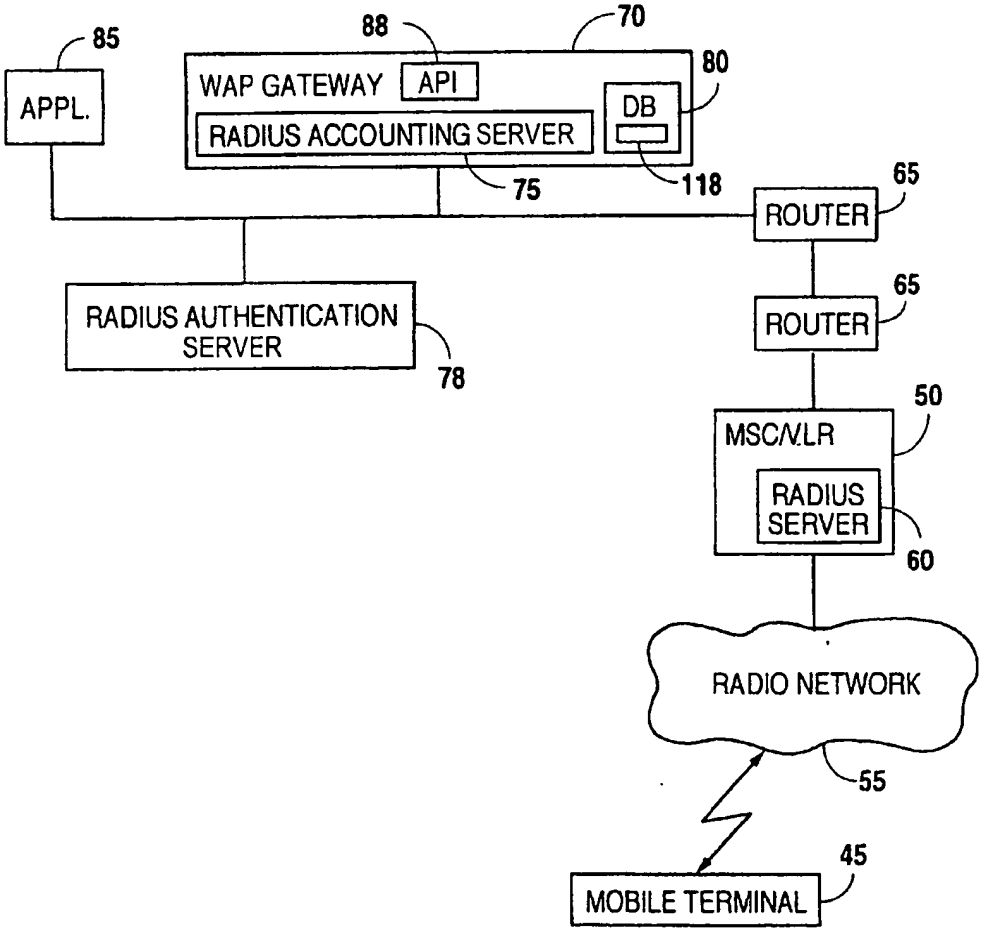
Publication Classification

(51) **Int. Cl.**[7] **G06F 15/16**

(52) **U.S. Cl.** **709/227**; 709/232

(57) **ABSTRACT**

In one embodiment, there is disclosed a system and method for providing access to an IP number or a subscriber identity number associated with a mobile device in a network, the method comprising associating a mobile device with a subscriber identity number; generating a temporary IP number for the mobile device; linking the subscriber identity number with the temporary IP number; storing the subscriber identity number and the temporary IP number in a database; and providing a pull application program interface to extract from the database either the subscriber identity number or the IP address for mobile device when requested by an application program.



US 20010028636A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2001/0028636 A1

Skog et al. (43) Pub. Date: Oct. 11, 2001

(54) METHOD AND APPARATUS FOR MAPPING AN IP ADDRESS TO AN MSISDN NUMBER WITHIN A SERVICE NETWORK

(76) Inventors: Robert Skog, Hasselby (SE); Ingvar Berg, Nykil (SE)

Correspondence Address:
Brian D. Walker
Jenkens & Gilchrist, P.C.
3200 Fountain Place
1445 Ross Avenue
Dallas, TX 75202-2799 (US)

(21) Appl. No.: 09/802,521

(22) Filed: Mar. 9, 2001

Related U.S. Application Data

(63) Non-provisional of provisional application No. 60/188,437, filed on Mar. 10, 2000. Continuation-in-part of application No. 09/596,802, filed on Jun. 19, 2000.

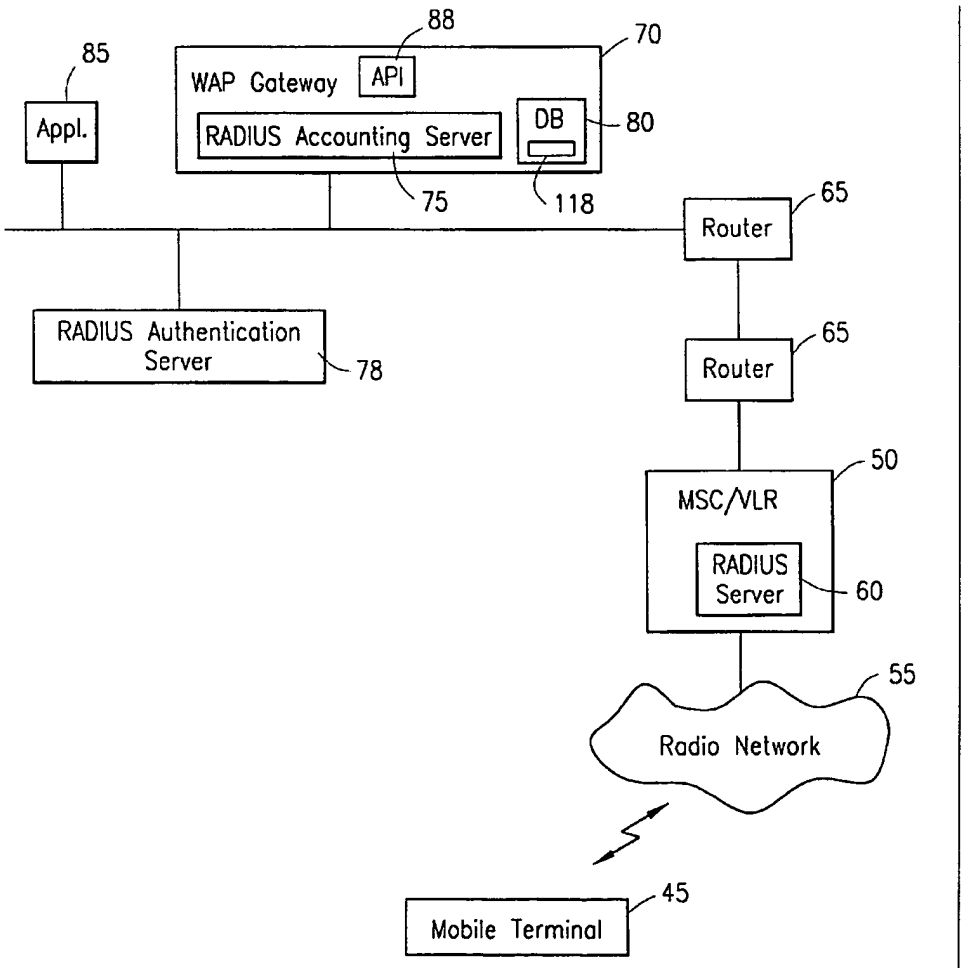
Publication Classification

(51) Int. Cl.[7] H04Q 7/00; H04L 12/28; H04L 12/56

(52) U.S. Cl. 370/328; 370/401

(57) ABSTRACT

A system and method for associating an MSISDN of a mobile terminal with a temporarily assigned IP address is disclosed. A first server located within a wireless communications network generates and transmits a start packet to a service network responsive to an access request by a mobile terminal. The start packet includes the MSISDN of the mobile terminal and an assigned IP address. A second server within the service network extracts the MSISDN in the IP address from the received start packet and stores this information together within a database. When a service request is made by the mobile terminal to a server n the service network, the MSISDN may be determined from the database and used to access user parameters in a user database



31/3,K/8 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014350529 **Image available**
WPI Acc No: 2002-171232/200222
Related WPI Acc No: 2004-167977
XRPX Acc No: N02-130273
System for using an Internet protocol address as a wireless **unit identifier for use at an** access point **to create a packet** identifying **the Internet** protocol **address**
Patent Assignee: QUALCOMM INC (QUAL-N)
Inventor: BENDER P E; BENDER P
Number of Countries: 096 Number of Patents: 014
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200156254	A1	20010802	WO 2001US2748	A	20010126	200222	B
AU 200134605	A	20010807	AU 200134605	A	20010126	200222	
NO 200203568	A	20020726	WO 2001US2748	A	20010126	200275	
			NO 20023568	A	20020726		
EP 1250791	A1	20021023	EP 2001906732	A	20010126	200277	
			WO 2001US2748	A	20010126		
BR 200107828	A	20030114	BR 20017828	A	20010126	200309	
			WO 2001US2748	A	20010126		
KR 2002082215	A	20021030	KR 2002709560	A	20020725	200319	
CN 1401178	A	20030305	CN 2001804147	A	20010126	200338	
JP 2003521167	W	20030708	JP 2001554587	A	20010126	200347	
			WO 2001US2748	A	20010126		
TW 521531	A	20030221	TW 2001101638	A	20010320	200364	
MX 2002007164	A1	20030101	WO 2001US2748	A	20010126	200373	
			MX 20027164	A	20020723		
US 6671735	B1	20031230	US 2000494204	A	20000128	200402	
AU 782376	B2	20050721	AU 200134605	A	20010126	200553	
MX 226242	B	20050211	WO 2001US2748	A	20010126	200565	
			MX 20027164	A	20020723		
EP 1250791	B1	20060118	EP 2001906732	A	20010126	200607	
			WO 2001US2748	A	20010126		

Priority Applications (No Type Date): US 2000494204 A 20000128
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200156254	A1	E	18	H04L-029/06	
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW					
AU 200134605	A			H04L-029/06	Based on patent WO 200156254
NO 200203568	A			H04L-000/00	
EP 1250791	A1	E		H04L-029/06	Based on patent WO 200156254
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR					
BR 200107828	A			H04L-029/06	Based on patent WO 200156254
KR 2002082215	A			H04L-012/28	
CN 1401178	A			H04L-029/06	
JP 2003521167	W		22	H04L-012/56	Based on patent WO 200156254
TW 521531	A			H04Q-007/24	
MX 2002007164	A1			H04L-029/06	Based on patent WO 200156254
US 6671735	B1			G06F-015/173	
AU 782376	B2			H04L-029/06	Previous Publ. patent AU 200134605

Based on patent WO 200156254
MX 226242 B H04L-029/06 Based on patent WO 200156254
EP 1250791 B1 E H04L-029/06 Based on patent WO 200156254
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

System for using an Internet protocol address as a wireless **unit identifier for use at an** access point **to create a packet** identifying **the Internet** protocol **address**

Abstract (Basic):
... Network **access points** (40) are distributed throughout a service area and **each** has **one** or more antennas to provide a corresponding coverage area which abuts **one** or more coverage areas. A packet **router** (42) provides interconnection between the **access points** and **assigns** a **unique** Internet protocol (IP) address to **each access point** for the IP packets, which is identified at the first point. The message is parsed to determine the address and a packet is created with the **design**ated address.
... AN **INDEPENDENT** CLAIM is included for a method of providing **wireless** services...

...Using an IP address as a **wireless** unit identifier...

...Network **access points** (40...

...Packet **router** (42...
...Title Terms: **WIRELESS** ;
International Patent Class (Main): **G06F-015/173** ...

... **H04L-000/00** ...

... **H04L-012/28** ...

... **H04L-012/56** ...

... **H04L-029/06** ...

... **H04Q-007/24**
International Patent Class (Additional): **H04L-012/66**
Manual Codes (EPI/S-X): **T01-C03C** ...

... **T01-H07A2** ...

... **T01-H07C5A** ...

... **T01-H07C5E** ...

... **T01-H07P** ...
... **W01-A06B7** ...

... **W01-A06C4** ...

... **W01-A06E1** ...

... **W01-A07G** ...

... **W01-B05** ...

... **W01-B05A1B** ...

US006671735B1

(12) **United States Patent**
Bender

(10) **Patent No.: US 6,671,735 B1**
(45) **Date of Patent: Dec. 30, 2003**

(54) **SYSTEM AND METHOD FOR USING AN IP ADDRESS AS A WIRELESS UNIT IDENTIFIER**

(75) Inventor: **Paul E. Bender**, San Diego, CA (US)

(73) Assignee: **Qualcomm Incorporated**, San Diego, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/494,204**

(22) Filed: **Jan. 28, 2000**

(51) **Int. Cl.**[7] **G06F 15/173**
(52) **U.S. Cl.** **709/238**; 370/351
(58) **Field of Search** 709/238, 245; 370/338, 356, 351

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,953,322	A	*	9/1999	Kimball	370/328
6,061,341	A	*	5/2000	Andersson et al.	370/338
6,151,319	A	*	11/2000	Dommety et al.	370/395.52
6,154,461	A	*	11/2000	Sturniolo et al.	370/401
6,167,040	A	*	12/2000	Haeggstrom	370/352
6,233,608	B1	*	5/2001	Laursen et al.	709/217
6,236,653	B1	*	5/2001	Dalton et al.	370/352
6,252,952	B1	*	6/2001	Kung et al.	379/114.1
6,308,273	B1	*	10/2001	Goertzel et al.	713/201
6,314,108	B1	*	11/2001	Ramasubramani et al.	370/465
6,373,930	B1	*	4/2002	McConnell et al.	379/114.28
6,374,108	B1	*	4/2002	Jakobsen et al.	455/432.1
6,449,269	B1	*	9/2002	Edholm	370/352
6,457,039	B1	*	9/2002	Fogelholm et al.	709/200
6,487,406	B1	*	11/2002	Chang et al.	455/422.1
6,487,605	B1	*	11/2002	Leung	709/245
2001/0012282	A1	*	8/2001	Yegoshin	370/338
2001/0038626	A1	*	11/2001	Dynarski et al.	370/356
2002/0105934	A1	*	8/2002	Lee et al.	370/338
2002/0161927	A1	*	10/2002	Inoue et al.	709/245

FOREIGN PATENT DOCUMENTS

DE	1 014 628	A1 *	6/2000	H04L/7/26
EP	0938217	A2	8/1999	
EP	1014628	A1	6/2000	
JP	WO99/59301	*	11/1999	H04L/12/56
US	WO 0024166	*	4/2000	H04L/12/66
WO	00/41376		7/2000	

OTHER PUBLICATIONS

Lee et al., "The Next Generation of the Internet: Aspect of the Internet Protocol Version 6" IEEE, Jan. 1998, pp. 28–33.*

Danny Cohen et al., "IP Addressing and Routing in a Local Wireless Network," Florence, May 4–8, 1992, New York, IEEE, US, vol. Conf. 11, 1992 (pp. 626–632).

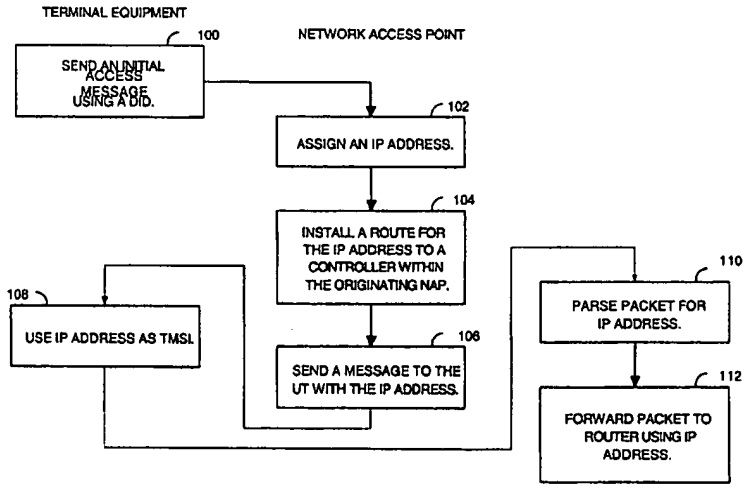
* cited by examiner

Primary Examiner—Bunjob Jaroenchonwanit
(74) *Attorney, Agent, or Firm*—Philip Wadsworth; Kent Baker; Sandra L. Godsey

(57) **ABSTRACT**

A first network access point receives a first wireless link message from a first user terminal. The first wireless link message identifies the first user terminal. The first network access point or other system entity assigns an IP address to the first user terminal for use as a temporary mobile station identifier. The first network access point or other system entity installs a route for the IP address to a controller. The first network access point forwards a wireless link message to the user terminal specifying the IP address. The first or a second network access point receives another wireless link message from the first user terminal in which the first user terminal is identified with the IP address. The first or second network access point parses the message to determine the IP address and creates at least one standard IP packet designating the IP address specified in the message. The first or second network access point forwards the message to a router which routes the packet according to the IP address.

6 Claims, 3 Drawing Sheets



nating network access point **40**. For example, depending on the manner in which the IP address is selected, a static or dynamic route for the IP address is established according to well-known techniques. The network access point **40** informs the user terminal **46** of the selected IP address in a message, which designates both the DID and the IP address.

From this point forward in the communication protocol, the user terminal **46** uses the IP address as the MSID. For example, the user terminal **46** sends messages on the access, control, or traffic channels specifying the selected IP address.

In one embodiment, whenever a new or originating network access point **40** receives a message from the user terminal **46**, the network access point **40** parses the message to determine the IP address. The network access point **40** creates an IP packet using the IP address as the address. The network access point **40** passes the packet to the packet router **42**, which routes the packet according to the IP address. In this way, it is not necessary for a new network access point **40** to access a system-wide memory bank to determine the routing of an incoming packet. Instead, the network access points **40** rely solely on the information received in the packet. The system automatically forwards the IP packet to the appropriate network access controller using well-known techniques.

FIG. **3** is a flow chart illustrating operation in accordance with one embodiment. In block **100**, a user terminal sends an initial access message to a network access point specifying a dummy identifier. In block **102**, an IP address is assigned to the user terminal for use during this session. Note that at this time, the network access point may not know the actual identity of the user terminal. In one embodiment, the IP address can be chosen by a dynamic host control processor. Alternatively, the network access point may select the IP address from a static pool. In block **104**, a route is installed for the IP address according to wellknown principles. For example, a route is established which routes the IP address to a controller or control functionality within the original network access point. In general, a route is established to a controller configured to control the operation of the user terminal throughout the current session such as to provide control point functionality; and the controller may be located within a variety of system elements.

In block **106**, the network access point sends a message to the user terminal using the dummy identifier as the MSID and specifying the designated IP address within the message. In block **108**, the user terminal uses the IP address as a MSID and sends a message to the network access point. For example, in one embodiment, the message is a registration message. In another embodiment, the message carriers other overhead information or user data. In block **110**, the network access point parses the message to determine the IP address. In block **112**, the original network access point forwards a corresponding message to the router using the IP address as the source address.

In a similar manner, other entities coupled to the router can send messages to the user terminal using the IP address. The messages are routed to the original network access point which maintains identification information for the user terminal. For example, if a second network access point receives a message from the user terminal, the second network access point creates a corresponding message using the IP address as the destination address and forwards the message to the router. For example, referring also to FIG. **2**, assume that steps **100**, **102**, **104**, and **106** have been performed so that the user terminal **46** has been assigned an IP address and a corresponding route has been established to a controller assigned to the user terminal **46**. Also assume that the network access point **40B** is the originating network access point and that that controller is within the network access point **40B**. Also assume that the current the user terminal **46** is within the coverage area of the network access point **40A**. When the user terminal **46** creates a message, it creates a message identifying itself using the IP address. The message can be created according to the corresponding wireless link protocol. The message is forwarded to the network access point **40A** such as over a wireless link path **60**. The network access point **40A** parses the message to determine the IP address. The network access point **40A** creates a packet using the IP address as the destination address. The network access point **40A** forwards the message to the packet router **42** such as over a standard IP path **62**. The packet router **42** routes the packet to the controller within the network access point **40B** such as over a standard IP path **64**.

The above-described methods and apparatuses are particularly advantageous when used in conjunction with a system such as the QUALCOMM® HDR-2000 generally referred to as "QUALCOMM® High Data Rate Air Interface" and IS-95. In these systems, a 32-bit MSID is specified. Because the IP address is also 32 bits, the use of an IP address as a MSID is particularly advantageous in these embodiments.

The invention may be implemented in a variety of media including software and hardware. Typical embodiments of the invention comprise computer software which executes on a standard microprocessor, discrete logic, or an application specific integrated circuit (ASIC.)

The invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiment is to be considered in all respects only as illustrative and not restrictive and the scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed is:

1. A method of providing wireless services comprising:

receiving a first wireless link message at a first network access point, the first wireless link message from a first user terminal, the first wireless link message identifying the first user terminal;

assigning an IP address to a controller within an access network, the IP address used for controlling operation of the first user terminal, the controller storing a current state of a communication session for the first user terminal;

assigning the IP address to the first user terminal for use as a mobile station identifier, the IP address being designated to a controller for controlling operation of the first user terminal throughout a communication session;

installing a route for the IP address to the controller;

forwarding a second wireless link message to the user terminal specifying the IP address;

receiving a third wireless link message from the first user terminal wherein the first user terminal is identified with the IP address, and

routing the third wireless link message to the controller using the IP address.

2. The method of claim **1** further comprising parsing the third message to determine the IP address of the controller and creating at least one standard IP packet designating the IP address.

3. A system for providing wireless service comprising:

a packet router; and

a first network access point corresponding to a first coverage area, the first network access point coupled to the packet router and comprising:

means to receive wireless link signals from a user terminal within the first coverage area;

means to establish a route within the packet router for an IP address, the IP address corresponding to control functionality within the first network access point;

means to assign the IP address as a Mobile Station Identifier for the user terminal; and

means to receive messages from the user terminal Identified by the IP address as a Mobile Station Identifier (MSID), and route the messages to the network access point using the IP address.

4. The system of claim 3 further comprising a second network access point coupled to the packet router, the second network access point comprising:

means to receive wireless link messages from the user terminal within a second coverage area;

means to parse the wireless link message to determine the IP address; and

means to create a standard IP packet designating the IP address and pass the standard IP packet to the packet router.

5. A system for providing wireless services comprising the steps of:

means for receiving a first wireless link message at a first network access point, the first wireless link message from a first user terminal, the first wireless link message identifying the first user terminal;

means for assigning an IP address to the first user terminal for use as a Mobile Station Identifier (MSID), the IP address being assigned to a controller at the first network access point, the controller for controlling operation of the first user terminal throughout a communication session, wherein the controller stores a current state of the communication session for the first user terminal;

means for installing a route for the IP address to a controller;

means for forwarding a second wireless link message to the user terminal specifying the IP address; and

means for receiving a third wireless link message from the first user terminal wherein the first user terminal Is identified with the IP address as the MSID.

6. A network access point in a wireless communication system, the network access point adapted for communication with an Internet Protocol (IP) network, the network access point comprising:

a receiver adapted to receive a message from a user terminal and parse the message to determine an IP address of the user terminal, the IP address being used as a Mobile Station Identifier (MSID) and as a destination IP address of a controller of an originating access point for the user terminal;

controller for radio link layer management, signaling protocol management, and data link layer management over a wireless link;

means for creating an IP packet using the IP address as the address;

means for passing the packet to a packet router, which routes the packet according to the IP address.

* * * * *

31/3,K/38 (Item 38 from file: 350)
DIALOG(R)File 350:Derwent WPIX

009230167 **Image available**
WPI Acc No: 1992-357589/199243
XRPX Acc No: N92-272523
Service provision authentication protocol **for** radiotelephone - **using service provider which feeds secret** assigned **to** particular cellular **telephone, random number and other data into same hash function**
Patent Assignee: AT & T CORP (AMTT); AMERICAN TELEPHONE & TELEGRAPH CO (AMTT); AT & T BELL LAB (AMTT)
Inventor: REEDS J A; TREVENTI P A
Number of Countries: 007 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5153919	A	19921006	US 91759311	A	19910913	199243	B
EP 532231	A2	19930317	EP 92308004	A	19920903	199311	
FI 9204091	A	19930314	FI 924091	A	19920911	199324	
JP 6195024	A	19940715	JP 92267811	A	19920911	199433	
EP 532231	A3	19940427	EP 92308004	A	19920903	199523	
EP 532231	B1	20000809	EP 92308004	A	19920903	200039	
DE 69231327	E	20000914	DE 631327	A	19920903	200053	
			EP 92308004	A	19920903		
FI 108689	B1	20020228	FI 924091	A	19920911	200223	

Priority Applications (No Type Date): US 91759311 A 19910913
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5153919	A		16	H04L-009/00	
EP 532231	A2	E	17	H04L-009/32	
Designated States (Regional): DE FR GB SE					
FI 9204091	A			H04K-001/06	
JP 6195024	A		13	G09C-001/00	
EP 532231	B1	E		H04L-009/32	
Designated States (Regional): DE FR GB SE					
DE 69231327	E			H04L-009/32	Based on patent EP 532231
FI 108689	B1			H04K-001/02	Previous Publ. patent FI 9204091

Service provision authentication protocol **for** radiotelephone - ...

...**using service provider which feeds secret** assigned **to** particular cellular **telephone, random number and other data into same hash function**

...Abstract (Basic): When a **cellular** telephone first enters the jurisdiction of a **base station** , it registers itself with the station by concatenating a secret password and the most recently...
...The service provider, upon learning of the **cellular** telephone's identity, feeds the secret **assigned** to that telephone and the random number, along with other information, into the same hash...

...The provider sends the cell a shared secret data field which is known to the **mobile** unit, and subsequent authentication processes are carried out between the unit and the cell itself...

...ADVANTAGE - Prevents piracy of **cellular** services...
...Title Terms: **RADIOTELEPHONE** ;
...International Patent Class (Main): **H04L-009/00** ...

... **H04L-009/32**
...International Patent Class (Additional): **H04L-009/20** ...

... **H04Q-007/20**
Manual Codes (EPI/S-X): **W01-A05** ...

... **W01-C01D3A** ...

... **W02-L**

US005153919A

United States Patent [19]

Reeds, III et al.

[11] Patent Number: 5,153,919

[45] Date of Patent: Oct. 6, 1992

[54] SERVICE PROVISION AUTHENTICATION PROTOCOL

[75] Inventors: James A. Reeds, III, New Providence; Philip A. Treventi, Murray Hill, both of N.J.

[73] Assignee: AT&T Bell Laboratories, Murray Hill, N.J.

[21] Appl. No.: 759,311

[22] Filed: Sep. 13, 1991

[51] Int. Cl.[5] H04L 9/00

[52] U.S. Cl. 380/44; 380/21; 380/23

[58] Field of Search 380/23, 25, 21, 44

[56] References Cited

U.S. PATENT DOCUMENTS

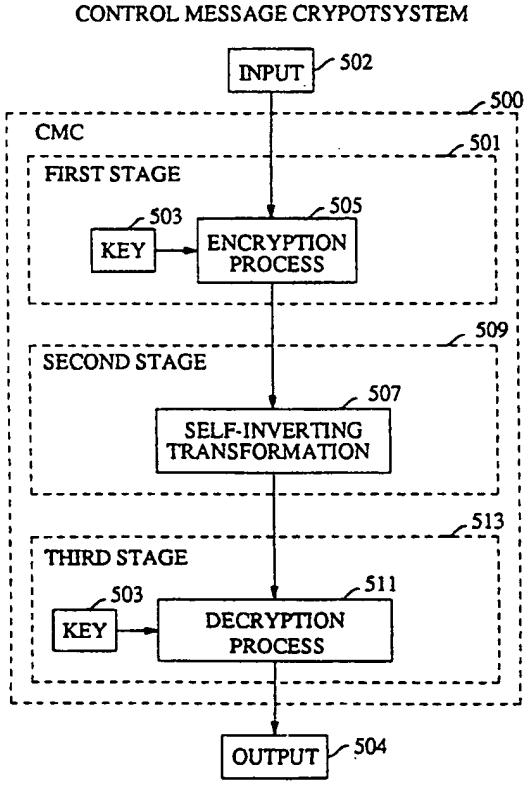
4,555,805	11/1985	Talbot	380/23
4,658,093	4/1987	Hellman	380/25
4,811,377	3/1989	Krolopp et al.	380/23
4,995,083	2/1991	Baker et al.	380/23
5,077,790	12/1991	D'Amico et al.	380/23

Primary Examiner—Salvatore Cangialosi
Attorney, Agent, or Firm—H. T. Brendzel

[57] ABSTRACT

A protocol for authenticating a cellular telephone to a service provider for the purpose of preventing the piracy of cellular services. A service provider assigns a unique "secret", along with other information such as a telephone number, to each cellular telephone when the telephone service is established with the service provider. Each base station of a service provider continuously broadcasts a periodically changing random number to all of the cellular telephones within the base station's jurisdiction. When a cellular telephone first enters the jurisdiction of a base station, it registers itself with the base station by concatenating a secret password and the most recently broadcast random number, along with other information, and passing the concatenated information to a hash function. The cellular telephone then sends the output of the hash function, along with other identifying information to the service provider. The service provider, upon learning of the cellular telephone's identity, feeds the secret assigned to that cellular telephone and the random number, along with other information, into the same hash function. When the result of the hashing performed by the service provider matches that provided by the cellular telephone, authentication for that cellular telephone is complete. Thereupon, the provider sends the cell a shared secret data field which is known to the mobile unit, and subsequent authentication processes are carried out between the mobile unit and the cell itself.

39 Claims, 7 Drawing Sheets



II. The second stage of CMC is:
1. for all values of i in the range $0 \leqq i < (d-1)/2$: $b(i) = b(i) \ominus (b(d-1-i)$ OR 1), where OR is the bitwise boolean OR operator.

III. CMC's final stage is the decryption that is inverse of the first stage:
1. Initialize a variable z to zero,
2. For successive integer values of i in the range $0 \leqq i < d$
   a. form a variable q by: $q = z \ominus$ low order byte of i,
   b. form variable k by: k=TBOX[q],
   c. update z with: $z = b(i) + z \bmod 256$,
   d. update b(i) with: $b(i) = b(i) - k \bmod 256$.

The three stage process employed to encrypt and decrypt selected control and data messages is illustrated in FIG. 10. In one preferred embodiment the first stage and the third stage are an autokey encryption and decryption, respectively. An autokey system is a time-varying system where the output of the system is used to affect the subsequent output of the system. For further reference regarding cryptography and autokey systems, see W. Diffie and M. E. Hellman, *Privacy and Authentication: An Introduction to Cryptography*, Proc. of the I.E.E.E., Vol. 67, No. 3, March 1979.

Mobile Unit Apparatus

FIG. 11 presents a block diagram of a mobile unit hardware. It comprises a control block **200** which includes (though not illustrated) the key pad of a cellular telephone, the hand set and the unit's power control switch. Control block **200** is connected to processor **210** which controls the workings of the mobile unit, such as converting speech signals to digital representation, incorporating error correction codes, encrypting the outgoing digital speech signals, decrypting incoming speech signals, forming and encrypting (as well as decrypting) various control messages, etc. Block **210** is coupled to block **220** which comprises the bulk of the circuitry associated with transmission and reception of signals. Blocks **200-220** are basically conventional blocks, performing the functions that are currently performed by commercial mobile telephone units (though the commercial units do not carry out encrypting and decrypting). To incorporate the authentication and encryption processes disclosed herein, the apparatus of FIG. 11 also includes a block **240** which comprises a number of registers coupled to processor **210**, and a "personality" module **230** that is also coupled to processor **210**. Module **230** may be part of the physical structure of a mobile telephone unit, or it may be a removable (and pluggable) module that is coupled to the mobile telephone unit through a socket interface. It may also be coupled to processor **210** through an electromagnetic path, or connection. In short, module **230** may be, for example, a "smart card".

Module **230** comprises a Jumble processor **231** and a number of registers associated with processor **231**. Alternately, in another preferred embodiment, only the A-Key is in the module **230**. A number of advantages accrue from installing (and maintaining) the A-key, and the MIN1 and MIN2 designations in the registers of module **230**, rather than in the registers of block **240**. It is also advantageous to store the developed SSD field in the registers of module **230**. It is further advantageous include among the registers of module **230** any needed working registers for carrying out the processes of processor **231**. By including these elements in module **230**, the user may carry the module on his person to use it with different mobile units (e.g. "extension" mobile units) and have none of the sensitive information be stored outside the module. Of course, mobile units may be produced with module **230** being an integral and permanent part of the unit. In such embodiments, Jumble processor **231** may be merged within processor **210**. Block **240** stores the unit's ESN designation and the various RAND sequences that are received.

Although the above disclosure is couched in terms of subscriber authentication in a cellular telephony environment, and that includes personal communication networks which will serve portable wallet sized handsets, it is clear that the principles of this invention have applicability in other environments where the communication is perceived to be not sufficiently secure and where impersonation is a potential problem. This includes computer networks, for example.

We claim:

1. A method, carried out by a customer unit that maintains a code sequence, for establishing a communications channel with a base station, comprising the steps of:
receiving from the base station a digital signal sequence;
developing a string which includes the code sequence, the digital signal sequence, and a sequence of bits that is characteristic of the customer unit;
hashing the string to develop a hashed string; and
using the hashed string in further communications with the base station.

2. The method of claim **1** wherein said sequence of bits that is characteristic of the customer unit includes a bit string that is unique to the customer unit hardware (ESN designation) and a bit string that is assigned to said unit as a customer of a service provider (MIN designation).

3. The method of claim **1** wherein said step of developing the hashed string is carried out pursuant to a directive from said base station.

4. The method of claim **1** including a step of initiating the steps of receiving, developing, hashing and using said hashed string when said base station desires to direct said customer unit to create a replacement for said hashed string.

5. The method of claim **1** further comprising the step of enciphering customer data signals with the aid of a portion of said hashed string.

6. The method of claim **1** wherein said step of using the hashed string in further communication employs the hashed string in a plurality of communications sessions through the communication channel.

7. The method of claim **1** further comprising the steps of:
creating a challenge string,
transmitting the challenge string,
forming an authentication string that comprises the challenge string, said sequence of bits that is characteristic of the customer unit, and at least a portion of the hashed string;
hashing the authentication string to form a hashed authentication string;
receiving a verification string in response to said step of transmitting the challenge string;
comparing the received verification string with the hashed authentication string; and
transmitting results of said step of comparing.

8. The method of claim **1** further comprising a step of verifying that the base station recognizes the hashed

string developed by said customer unit to be a valid hashed string.

9. The method of claim 8 wherein said step of verifying comprises the steps of:

developing a challenge sequence;

sending said challenge sequence to said base station;

forming an authentication string from a concatenation of said challenge sequence, said hashed string and selected other information;

hashing said authentication string to form a hashed authentication string;

receiving a hashed signal from said base station that is related to said challenge sequence sent to said base station;

comparing said hashed authentication string with said hashed signal; and

reporting to said base station results of said step of comparing.

10. A method, carried out by a customer unit that maintains a code sequence, for establishing a communications channel with a base station, comprising the steps of:

receiving from the base station a digital signal sequence;

developing a string which includes the digital signal sequence, a sequence of bits that is characteristic of said customer unit and a key derived from the code sequence;

hashing the string to develop a hashed string; and

sending the hashed string to the base station.

11. The method of claim 10 wherein said base station has no knowledge of said code sequence.

12. The method of claim 10 wherein the sequence of bits is nonsecret.

13. The method of claim 10 wherein the customer unit is mobile and the base station is non-mobile.

14. The method of claim 10 wherein the established communication channel is a wireless communication channel.

15. The method of claim 10 wherein the established communication channel is a cellular radio communication channel.

16. The method of claim 10 further comprising the steps of determining that the mobile customer unit has entered the jurisdiction of the base station.

17. The method of claim 10 wherein said step of sending the hashed string also sends at least a portion of said string.

18. The method of claim 10 including a step of initiating the steps of receiving, developing, hashing and sending said hashed string when said customer unit desires to initiate a call.

19. The method of claim 10 including a step of initiating the steps of receiving, developing, hashing and sending said hashed string when said base station desires to activate said customer unit to receive a call.

20. The method of claim 10 including a step of initiating the steps of receiving, developing, hashing and sending said hashed string when said base station desires to re-authenticate said customer unit.

21. A method, carried out by a customer unit that maintains a code sequence, for establishing a communications channel with a base station that has no knowledge of said code sequence, comprising the steps of:

(a) receiving from said base station a digital signal sequence;

(b) developing a string which includes

(1) a substring containing a sequence of bits that is characteristic of said customer unit,

(2) a substring that is related to a specified action to be taken by said customer unit, which substring is selected from a set comprising

(i) a null string,

(ii) a string of bits corresponding to a number assigned to said customer unit, and

(iii) a string corresponding to the number of another customer unit to which connection is sought,

(3) a substring containing said digital signal sequence, and

(4) a substring containing a key derived from said code sequence;

(c) hashing said string to develop a hashed string; and

(d) sending said hashed string to said base station.

22. The method of claim 21 further comprising a step of receiving from said base station an indication of the action to be taken by said customer unit.

23. The method of claim 21 wherein the sequence of bits that is characteristic of the customer units comprises the customer unit's phone number.

24. The method of claim 21 wherein the sequence of bits that is characteristic of the customer units comprises the customer unit's electronic serial number.

25. A customer unit for communicating with a system, said customer unit including first means (200) for developing call initiation control signals and call progress control signals second means (210, 230, 240) responsive to said call initiation control signals and call progress control signals for establishing and maintaining a communication channel with said system in accordance with a protocol third means (200) for creating data signals, and fourth means (220) for applying the data signals and the call control signals to said communication channel, said second means CHARACTERIZED BY:

a processor responsive to said third means and said fourth means;

means A (a register in block 240) for developing an identifier signal that is unique to said customer unit;

means B for storing (240) a temporary string signal (RAND) received from said system;

means C for storing (232) an identifier signal (MIN) supplied by an owner of said system, a code sequence key signal (A-key) supplied by said owner of said system, an authentication key signal (SSD-A), and a speech encryption key signal (SSD-B);

means D (231) responsive to said processor for hashing an applied string and developing thereby a hashed output;

means E for applying said authentication key to means D.

26. The customer unit of claim 25 wherein said temporary string maintained in means B is repetitively updated from a signal provided by said fourth means.

27. The customer unit of claim 26 wherein the time duration between successive updates of said temporary string is less than the expected time duration between the application of call initiation control signals.

28. The customer unit of claim 25 wherein said processor, upon receipt of a signal from said fourth means that directs the creation of a new authentication key signal and a new speech key signal, applies hashed output signals of means D to means C to modify said authentication key signal and said speech key signal.

29. The customer unit of claim 28 wherein the hashed output of means D is a multi-bit binary word, one portion of said binary word constitutes said authentication key signal, and another portion of said binary word constitutes said speech key signal.

30. The customer unit of claim 25 wherein at least the portion of means C that stores the code sequence key signal is in a removable module.

31. The customer unit of claim 30 wherein said module is adapted to be connected to said processor via electrical contacts.

32. The customer unit of claim 30 wherein said module is adapted to be connected to said processor via electromagnetically coupled connections.

33. A method carried out by a communications system for establishing a communications channel with a customer unit comprising the steps of:

maintaining an authentication key of said customer unit;

receiving a first hashed authentication string from said customer unit;

forming a local authentication string by combining said authentication key with other information;

hashing said local authentication string to form a local hashed authentication string; and

comparing said local hashed authentication string with the first hashed authentication string.

34. The method of claim 33 further comprising the step of maintaining a designation of said customer unit that is provided to said system and is unique to said unit (MIN) and a code sequence designation of said customer unit (A-key).

35. The method of claim 34 further comprising the step of maintaining an ESN designation of said unit.

36. The method of claim 35 further comprising the steps of:

developing a number;

transmitting said number;

developing said authentication key by hashing a string comprising said number, said ESN designation and said code sequence designation of said customer unit in accordance with a hashing function.

37. The method of claim 33 further comprising the steps of

developing a number; and

broadcasting said number to said customer unit.

38. The method of claim 37 wherein said number is pseudorandom.

39. The method of claim 37 wherein said number is random.

* * * * *

31/3,K/41 (Item 41 from file: 350)
DIALOG(R)File 350:Derwent WPIX

007797565 **Image available**
WPI Acc No: 1989-062677/ **198909**
XRPX Acc No: N89-047828
PABX cordless telephone with security **checking-in** protocol - **has security check carried out on address code during call set-up protocols by micro-controller**
Patent Assignee: PHILIPS GLOEILAMPENFAB NV (PHIG)
Inventor: VAN DE MORTEL P P; VAN LOON J C F; LOON J C; MORTEL P P
Number of Countries: 010 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 304998	A	19890301	EP 88201771	A	19880818	198909	B
GB 2209109	A	19890426	GB 8720089	A	19870826	198917	
JP 1071331	A	19890316	JP 88209596	A	19880825	198917	
US 4905272	A	19900227	US 88235253	A	19880822	199015	
EP 304998	B1	19930707	EP 88201771	A	19880818	199327	
DE 3882182	G	19930812	DE 3882182	A	19880818	199333	
			EP 88201771	A	19880818		
KR 9702755	B1	19970310	KR 8810679	A	19880823	199935	

Priority Applications (No Type Date): GB 8720089 A 19870826
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 304998	A	E	8		
Designated States (Regional): CH DE FR GB IT LI SE					
US 4905272	A		8		
EP 304998	B1	E	11	H04M-001/72	
Designated States (Regional): CH DE FR GB IT LI SE					
DE 3882182	G			H04M-001/72	Based on patent EP 304998
KR 9702755	B1			H04Q-007/00	

PABX cordless telephone with security **checking-in** protocol -

...Abstract (Basic): The telephone system consists of a **base station** (10) connected to the public switching network serving five handsets by duplex **radio** links. Control of the system is by a micro-controller (16) in the base unit. **Each** handset has a micro-controller for control of the various functions in the handset and...

...in which is stored a multiple bit, say 16, security address code which is changed **each** time the handset is recharged. During call set-up protocols the **base station** carries out a security check on its associated handsets using, typically, 8 bits of the...
...ADVANTAGE - Prevents conflict between cordless PABX systems on the same **radio** frequency...
...Abstract (Equivalent): The telephone system consists of a **base station** (10) connected to the public switching network serving five handsets by duplex **radio** links. Control of the system is by a micro-controller (16) in the base unit. **Each** handset has a micro-controller for control of the various functions in the handset and...

...in which is stored a multiple bit, say 16, security address code which is changed **each** time the handset is recharged. During call set-up protocols the **base station** carries out a security check on its associated handsets using, typically, 8 bits of the...

...ADVANTAGE - Prevents conflict between cordless PABX systems on the same **radio** frequency. (8pp Dwg.No.1/7)

...Abstract (Equivalent): A PABX cordless telephone system comprises a **base station** (10) and a number of handset (HS1 to HS5). The **base station** is connected to the public switching network and communicates with **each** handset by way of a respective duplex **radio** link. The operation of the PABX system is controlled by a micro-controller (16) in the **base station** . Micro-controllers are also present in **each** of the handsets. Security in the **radio** communication via the duplex **radio** links is provided by **assigning** an n-bit security address code, where n for example comprises 16 bits, to **each** handset...

...require the transmission of the full n-bit security code. In the interim periods the **base station** (10) carries out a security check on the handsets forming its system...

International Patent Class (Main): **H04M-001/72** ...

... **H04Q-007/00**

...International Patent Class (Additional): **H04Q-003/62** ...

... **H04Q-007/04**

Manual Codes (EPI/S-X): **W01-B03** ...

... **W01-B07** ...

... **W01-C01D**

United States Patent [19]

Van de Mortel et al.

[11] **Patent Number: 4,905,272**

[45] **Date of Patent: Feb. 27, 1990**

[54] **PABX CORDLESS TELEPHONE SYSTEM**

[75] Inventors: **Petrus P. Van de Mortel; Johannes C. F. Van Loon**, both of Eindhoven, Netherlands

[73] Assignee: **U.S. Philips Corporation**, New York, N.Y.

[21] Appl. No.: **235,253**

[22] Filed: **Aug. 22, 1988**

[30] **Foreign Application Priority Data**

Aug. 26, 1987 [GB] United Kingdom 8720089

[51] **Int. Cl.**[4] **H04Q 7/04**

[52] **U.S. Cl.** **379/62**; 379/63

[58] **Field of Search** 379/62, 61, 63

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,689,812	8/1987	Hata	379/62
4,700,375	10/1987	Reed	379/61
4,742,560	5/1988	Arai	455/33

FOREIGN PATENT DOCUMENTS

0196834	10/1986	European Pat. Off.	

OTHER PUBLICATIONS

Communication from the European Patent Office in a corresponding application.

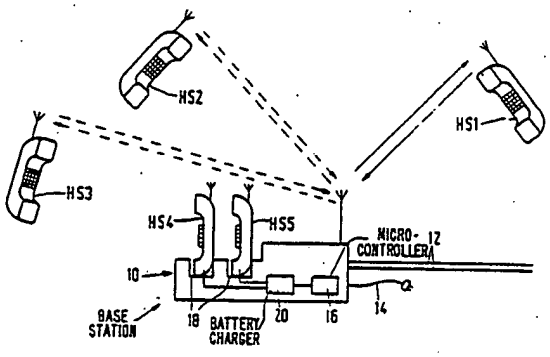
Primary Examiner—Robert Lev

Attorney, Agent, or Firm—Thomas A. Briody; Jack E. Haken; Anne E. Barschall

[57] **ABSTRACT**

A PABX cordless telephone system comprising a base station (**10**) and a plurality of handset (HS1 to HS5). The base station is connected to the public switching network and communicates with each handset by way of a respective duplex radio link. The operation of the PABX system is controlled by a micro-controller (**16**) in the base station. Micro-controllers are also present in each of the handsets. Security in the radio communication via the duplex radio links is provided by assigning an n-bit security address code, where n for example comprises 16 bits, to each handset. The signalling protocols in setting-up calls require the transmission of the full n-bit security code. In the interim periods the base station (**10**) carries out a security check on the handsets forming its system. Time, memory capacity in the micro-controllers and battery current can be saved while simultaneously achieving a high degree of security if the security check is carried out using m bits of the security codes where $m<n$ and m is typically equal to 8.

14 Claims, 3 Drawing Sheets



security code have been transmitted. Thereafter the micro-controller **62** activates the transmitter section of the handset and the security code is sent back to the base station micro-controller **16** via a radio link.

The old security code will be overwritten by the new security code once the transmitted and received code words are equal. Until that time the old code remains valid. Thus picking-up the handset during code transformation will have no consequence for the user because last written security code remains valid.

If the received code is not correct, the procedure will be repeated as long as the returned code is not equal to the code as transmitted by the base station. This technique is useful to confirm that the battery in the handset is recharged at least to an arbitrary minimum extent because there must be enough power in it to retransmit the security code back to the base station via the radio link. Cycling of successive security codes can take place every 9.4 ms.

Once a handset has been removed from a socket **18** (FIG. **1**) and is switched-on, security codes are transmitted to the base station **10**. The received codes are checked by the micro-controller **16** in the base station **10** and if equal, the base station transmitter is switched on and will send an acknowledgement signal. In order to allow time for checking the security code and switching-on of the transmitter oscillator **26** (FIG. **2**), a wait time of 20 ms is built-in before the acknowledgement is sent-out.

FIG. **5** illustrates a 25-bit code word **66** which is transmitted by the handset when it is switched on and a 4-bit acknowledgement signal **68** transmitted by the base station. The code word **66** comprises a synchrononisation bit **70**, eight bits **72** of information and a 16 bit security word **74**. This code word **66** is sent out by the handset at a speed of 115 bits/second. The handset waits for 64 ms and if an acklowledgement has not been received in the meantime then it repeats the sending of the code word **55** providing the handset is still on and an acknowledgement has been received. The acknowledgement signal comprises an instruction that dialling data is to be sent.

The dialling data has been formulated in accordance with a byte-oriented format to ensure the correct functioning of the entire system. The byte-oriented format comprises

(1) a first half byte,

(2) a second half byte, and

(3) subsequent bytes.

FIG. **6** illustrates a first code word transmitted by a handset to a base station. This code word is constituted by four parts. The first part comprises the 16-bit security address code **76**, the second part **78** comprises selection information for DTMF selection, if this form of dialling is available for use, the third part **80** comprises selection information for pulse dialling selection, if this form of dialling is available for use, and the fourth part **82** is the handset identification number of the calling party. For the purpose of synchronisation it is necessary for the first transmitted code word to be preceded by some synchronising pulses.

In the second code word the relevant dialling information is sent, for example the trunk-dialling code and the called party's number. In order to obviate the imperfections of the radio channel, redundancy has been used for transmission via the radio channel.

The receipt of these code words by the base station is acknowledged.

When the base station receives a call for one of its handsets, it transmits a code word comprising the 16 bit security code of the handset and, if applicable, the identification number of the handset. The identification number is necessary in those cases, there are two or more handsets forming extensions and each is allocated the same security number. The addressed handset acknowledges the receipt of the code word and at the same time causes its microphone amplifier and audio amplifier to be energized.

In a PABX system employing cordless telephones it is desirable for the base station to monitor the status of each the handsets, that is for example whether it is on standby, participating in a call involving the public switching network, or involved in an intercom call. In order to do this check the micro-controller interrogates each handset in turn using the control part of each channel, that is the FSK signalling centred on 7.0 kHz. In order to economise on the time taken in making the check bearing in mind the signalling rate of 115 bits per second and the desire to maintain a high degree of security the micro-controller **16** scans the channels sequentially by transmitting m of the n (where $n>m$) bits of the security code. This is illustrated in FIG. **7** of the drawings which assumes that the PABX has ten channels **C1** to **C10**. In the case of a **16** bit security code, $m=8$. The 8 bits may be the least significant bits of the code, the most significant bits or bits selected from a part intermediate the least and most significant bits. Security scanning using m out of n bits has an advantage over using the entire n bits because less buffer memory capacity has to be reserved in the base station micro-controller **16** and the memory capacity saved in this way is available for use in other operations by the micro-controller **16**. A further saving in time and memory capacity can be achieved by not carrying out a security check on those channels occupied by an intercom call. In any event the security check which it is desirable to make every one or two seconds can be completed in less than one second, more particularly in 80/115 seconds.

Battery current in the handsets is also saved by this measure because in the standby mode the receiver in each handset need only be switched-on for approximately half the time that a receiver has to be if n bits of security code are transmitted.

The handsets respond to the security check byte sending the same m bits as were transmitted by the base station together with an indication of their statuses. Once the response has been sent the transmitters in the handsets are switched-off.

In the event of a handset wishing to make a call or the base station receiving a call for a handset during the security check then the call set-up between the base station and the handset is delayed until the security check is completed. As the delay is less than one second than this is within the specification of many nationally approved telephone systems.

What is claimed is:

1. A PABX cordless telephone system comprising a base station and a plurality of disconnectable handsets, the base station and the handsets each having a respective transceiver for communication to and from each other by way of a respective duplex radio link, the base station having a micro-controller for controlling the system, and each handset having a respective micro-controller for controlling various functions in the handset, each respective micro-controller in the handsets including a respective memory for storing a respective

n-bit security address code which is used in call set-up protocol with the base station and the micro-controller in the base station including a memory for storing all the respective security address codes, wherein the micro-controller in the base station is programmed to carry out security checks on the handsets by using m bits of the respective security address codes where $m<n$.

2. A system as claimed in claim 1, wherein the security check is made using the m-least significant bits of each security address code.

3. A system as claimed in claim 1, wherein $n=16$ and $m=8$.

4. A system as claimed in claim 1, wherein

(a) each handset has a rechargeable battery,

(b) the base station has means for recharging the battery in place in each handset, the recharging means including battery charger contacts,

(c) the micro-controller in the base station includes a pseudo-random counter which is electrically coupled via the battery charger contacts and the rechargeable battery to the micro-controller in the handset so that the security address code of the handset is changed to a new security address code during recharging,

(d) the micro-controller in the handset causes its transceiver to transmit the new security address code via the duplex radio link to the base station,

(e) the micro-controller in the base station has means for comparing a received security code with the new security address code and if they are equal for instructing the security address code stored in the memories of the micro-controllers of the base station and the relevant handset to be overwritten by the new security address code.

5. A system as claimed in claim 1, wherein the security check by the base station micro-controller is effected by scanning its associated handsets in sequence.

6. A method of operating a PABX cordless telephone system comprising a base station and a plurality of handsets, each handset having an n-bit security address code which is also stored in the base station, wherein during call set-up protocols the full n-bit security codes are used in duplex radio links between the base station and the handsets and wherein the base station makes security checks on the handsets using m bits of the n-bit security code address, where $m<n$.

7. A method as claimed in claim 6, wherein the duplex radio links are scanned sequentially by the base station.

8. A method for operating a PABX cordless telephone system which includes a base station and a plurality of disconnectable handsets, each respective handset having a respective n-bit security address code which is stored in both the base station and in the respective handset, comprising the steps of:

a. transmitting the full n-bit security address codes in duplex radio links to and from the base station and the handsets, during call set-up protocols; and

b. making security checks of the handsets, in the base station, using m bits of the n-bit security address codes, where $m<n$.

9. A method as claimed in claim 6, wherein $n=16$ and $m=8$.

10. A system as claimed in claim 2, wherein $n=16$ and $m=8$.

11. A method as claimed in claim 8 comprising the step of carrying out signalling associated with the security checks in a first part of a channel frequency band above a second part of the channel frequency band, which second part is used for speech.

12. The method of claim 8 wherein the making step comprises using the m least significant bits of the security code addresses.

13. The method of claim 8 wherein the making step comprises signalling in a part of the channel frequency band above that used for speech.

14. The method of claim 8 further comprising the step of scanning the respective duplex radio links sequentially, said scanning step being performed by the base station and including one said transmitting step and one said making step for each respective duplex radio link.

* * * * *

24/3,K/15 (Item 15 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014234405 **Image available**
WPI Acc No: 2002-055103/200207
XRPX Acc No: N02-040678
Assigning unique identifiers for allowing communication between general packet radio **service system and remote authentication dial in user service server**
Patent Assignee: TELEFONAKTIEBOLAGET ERICSSON L M (TELF); AUNE L E (AUNE-I)
Inventor: AUNE L E
Number of Countries: 095 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200169858	A1	20010920	WO 2001SE469	A	20010306	200207	B
NO 200001316	A	20010917	NO 20001316	A	20000314	200207	
AU 200141322	A	20010924	AU 200141322	A	20010306	200208	
US 20020010683	A1	20020124	US 2001803022	A	20010312	200210	
NO 313950	B1	20021230	NO 20001316	A	20000314	200305	

Priority Applications (No Type Date): NO 20001316 A 20000314
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200169858	A1	E	13	H04L-012/28	
NO 200001316	A			H04L-012/66	
AU 200141322	A			H04L-012/28	Based on patent WO 200169858
US 20020010683	A1			G06F-015/16	
NO 313950	B1			H04L-012/66	Previous Publ. patent NO 200001316

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

Assigning unique identifiers for allowing communication between general packet radio **service system and remote authentication dial in user service server**

Abstract (Basic):
... One or more external networks are connected to a general packet **radio** service (GPRS) system by identifying each network with an **access point** name (APN) for **assigning** its **gateway** address. An APN-external network authentication request from a gateway GPRS support node (GGSN) is...
... In **RADIUS** -accounting communication for assigning **unique** identifiers allowing communication between a GPRS (General Packet **Radio** Service)-system and a RADIUS (Remote Authentication Dial In User Service) server...
...Title Terms: **RADIO** ;

US 20020010683A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2002/0010683 A1**

Aune (43) **Pub. Date: Jan. 24, 2002**

(54) **COMMUNICATION IDENTIFIER METHOD**

(76) Inventor: **Leif Einar Aune**, Grimstad (NO)

Correspondence Address:
NIXON & VANDERHYE P.C.
8th Floor
1100 North Glebe Rd.
Arlington, VA 22201-4714 (US)

(21) Appl. No.: **09/803,022**

(22) Filed: **Mar. 12, 2001**

(30) **Foreign Application Priority Data**

Mar. 14, 2000 (NO) 20001316

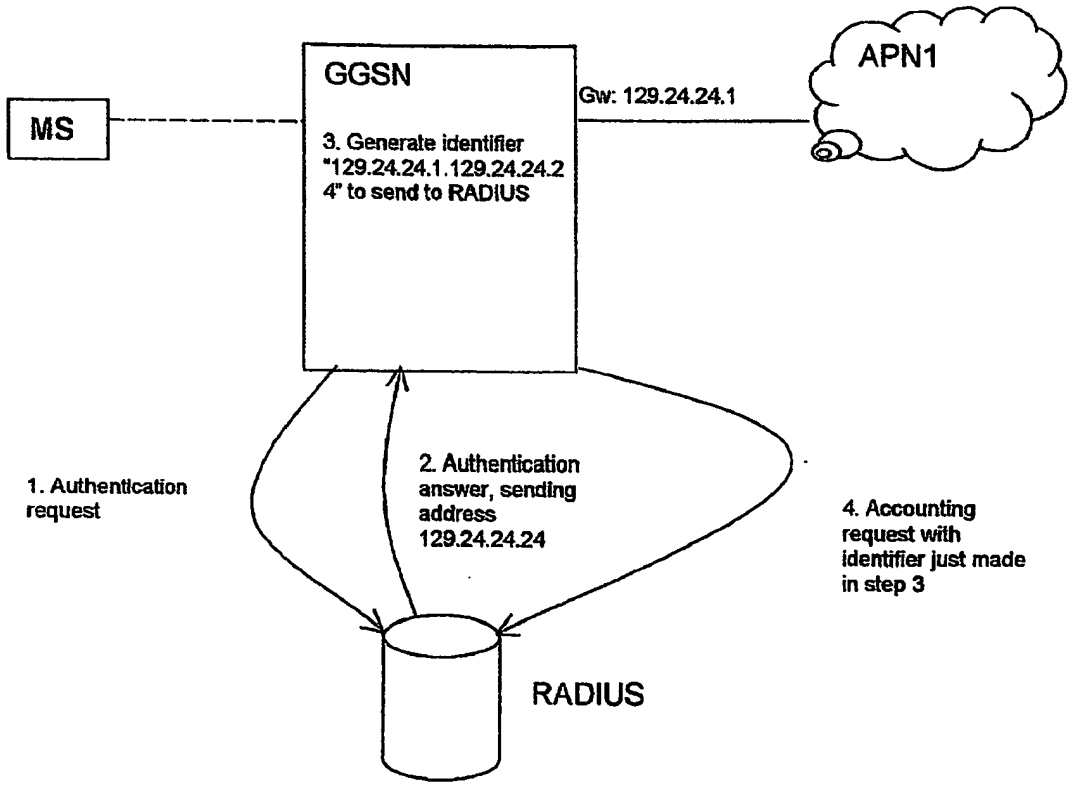
Publication Classification

(51) **Int. Cl.**[7] **G06F 15/16**

(52) **U.S. Cl.** **705/67**; 709/227

(57) **ABSTRACT**

A method for assigning unique identifiers for allowing communication between a GPRS (General Packet Radio Service) system and a RADIUS (Remote Authentication Dial In User Service) server. The method includes the steps of connecting one or more external networks to the GPRS system and identifying the or each network with an APN (Access Point Name), and assigning to an or each APN external network a gateway address. Further steps include passing an APN-external network authentication request from a GGSN (Gateway GPRS Support Node) to said RADIUS server, providing from said RADIUS server to said GGSN upon such request a subscriber IP (Internet Protocol) address to be stored in said GGSN (Gateway GPRS Support Node), said subscriber IP address being unique for the respective APN external network defined in said GGSN, using said GGSN for combining the APN gateway address and the subscriber IP address, to form a unique subscriber identifier, and sending from said GGSN said identifier to the RADIUS server for accounting, e.g. in the form of an ASCII string.



external network. By assuring that this IP-address is unique for each APN defined in the GGSN, all the external networks will have its own, unique identifier. Since two subscribers (MS) in the same external network should never use the same IP-address at the same time, subscribers connected to the same APN will always have different IP-addresses. The idea is to combine these two IP-addresses, the gateway-address for the APN and the address assigned to the subscriber, to form the identifier.

[0027] When the GGSN receives an IP-address to send to the subscriber from the RADIUS-server, it looks up the gateway-address belonging to the external net to which the subscriber is connecting himself. This address has already been configured when the external network is attached to the GPRS-system, and checked to be unique within the GGSN.

[0028] To construct the identifier to send to the RADIUS accounting-server the GGSN will now use these two available IP-addresses. The addresses can be appended to form a eight byte long identifier (in case of IP-addresses from IP version 4), or the numbers could be converted to ASCII numbers to make the string printable. When the numbers are converted it would be wise to insert dots (ASCII value 46) between the decimal-groups in the addresses to be able to clearly see the addresses used in the identifier (e.g. for an operator looking into the accounting records).

[0029] Gateway-address=129.24.24.1

[0030] MS IP-address=129.24.24.24

[0031] ASCII codes: 129 24 24 1 129 24 24 24 (non printable)

[0032] Or transform the number to ASCII codes for the numbers to make them printable:

[0033] ASCII codes: 49 50 57 46 50 52 46 50 52 46 49 46 49 50 57 46 50 52 46 50 52 46 50 52 (which would be readable as "129.24.24.1.129.24.24.24")

[0034] The identifier is suitably passed to the RADIUS server as an ASCII string. (See **FIG. 1**).

[0035] Thus, the gateway address is the address of the GPRS-system/GGSN as seen from the external network (APN, e.g. APN1) and the subscriber could be a mobile terminal MS connected to the external network through the GPRS-system.

[0036] On **FIG. 2**, the subscribers MS1, MS2 and MS3 have for sake of reference to their respective networks APN1, APN2 and APN3 been indicated on the right hand side of the drawing figure.

[0037] The APN name and the respective APN gateway address to the GGSN seen from the network are configured, as such new network is linked to the GPRS system. The operator will normally manually assign the APN name and the gateway address, and the RADIUS server is not involved in such operation.

[0038] **FIG. 2** shows three external networks connected to a GGSN node in a GPRS system. Each network has one subscriber connected and all the three networks use the same RADIUS server for authentication and dynamic IP-address allocation for the subscribers. Even though the networks identified as APN2 and APN3 has assigned the same IP-address to the two subscribers, the identifier will be unique because of the different gateway addresses. Table I shows the generated identifiers for the three subscribers.

TABLE 1

APN	Gateway Address	Subscriber IP Address	Identifier
APN1	129.24.24.1	129.24.24.24	"129.24.24.1.129.24.24.24"
APN2	193.25.01	193.25.5.1	"193.25.0.1.193.25.5.1"
APN3	193.26.0.1	193.25.5.1	"193.26.01.193.25.5.1"

[0039] Advantages

[0040] The creation of the identifier used for accounting purposes described above will not involve any new resources than the ones already available. Since the addresses already are unique, the combination of the two addresses will form a perfectly valid identifier. This will not restrict any limitations on concurrency regarding RADIUS accounting messages, and the identifier is guaranteed unique as long as the subscriber is still using the assigned IP-address (i.e. no accounting stop has been sent towards the RADIUS server). The creation of the identifier will not use any extra resources whatsoever, and will always be available as long as an IP-address exists.

[0041] The identifier will also be very predictable, and only by looking at this one can tell which external network the accounting record belongs to, as well as knowing the IP-address for the subscriber.

[0042] Whenever several IP-addresses are available, which together will identify the object in question uniquely, these addresses can be concatenated to form a unique identifier.

1. A method for assigning unique identifiers for allowing communication between a GPRS (General Packet Radio Service) system and a RADIUS (Remote Authentication Dial In User Service) server, the method including the steps of:

connecting one or more external networks to the GPRS system and identifying the or each network with an APN (Access Point Name), and

assigning to an or each APN external network a gateway address,

and the further steps of:

passing an APN-external network authentication request from a GGSN (Gateway GPRS Support Node) to said RADIUS server,

providing from said RADIUS server to said GGSN upon such request a subscriber IP (Internet Protocol) address to be stored in said GGSN (Gateway GPRS Support Node), said subscriber IP address being unique for the respective APN external network defined in said GGSN,

using said GGSN for combining the APN gateway address and the subscriber IP address, to form a unique subscriber identifier, and

sending from said GGSN said identifier to the RADIUS server for accounting, e.g. in the form of an ASCII string.

2. The method according to claim 1, wherein:

Two or more of said APN external networks are provided with same subscriber IP address, but different gateway addresses to yield different unique APN identifiers.

3. The method according to claim 1, wherein

Two or more subscribers are present in at least one of said networks, each subscriber in a common network being provided with its own subscriber IP address, but same network gateway address.

4. The method according to claim 1, wherein

The identifier is a code string having as a first element the gateway address of the APN external network in question and as a second element the subscriber IP address appended thereto.

* * * * *

31/3,K/20 (Item 20 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013098550 **Image available**
WPI Acc No: 2000-270422/200023
Related WPI Acc No: 2004-166852; 2004-281233
XRPX Acc No: N00-202508
Mobile **assisted handoff method in digital** cellular **communication, involves** identifying optimal candidate base station **by correlation identification code of candidate channel with received signal strength**
Patent Assignee: SBC TECHNOLOGY RESOURCES INC (SBCT-N)
Inventor: KOBYLINSKI R A; MAJMUNDAR M V
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6044272	A	20000328	US 97804658	A	19970225	200023	B

Priority Applications (No Type Date): US 97804658 A 19970225
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6044272	A		10	H04Q-007/20	

Mobile **assisted handoff method in digital** cellular **communication, involves identifying optimal candidate** base station **by correlation identification code of candidate channel with received signal strength**

Abstract (Basic):
... A measurement order comprising list of candidate channel is transmitted to **mobile** station. Based on received signal strength, optimum candidate channel is **selected** . Data within time window of channel is read and processed by searching **identification** (**ID**) codes. Then, the ID code is correlated with received signal measurements, to identify optimal candidate **base station** for effecting handoff.
... List of candidate channels are generated for possible acceptance of communication handoff between **mobile** and **base stations** . The current **base station** transmits a first measurement order containing list of candidate channels to **mobile** station, in which received signal strength corresponding to **each** candidate channel is listed in measurement order. Based on measured signal strength, most favorable candidate channel is **selected** . Then, another measurement order containing most favorable channel is transmitted to the **mobile** station. The candidate channel is tuned by reading data within time window on candidate channel...

...synchronization word within the read data. Then, the read data is stored in memory of **mobile** station, after which data is processed by searching identification code from first predetermined number of...

...of symbols. The identified code has digital voice color code word in candidate channel. The **mobile** station transmits the ID codes of **each** channel to current **base station** . The ID codes are correlated with received signal measurements, to identify an optimal candidate **base station** for effecting handoff of communication...

...To effect communication link between **mobile** and **base stations** in digital **cellular** communication network...

...Improves quality of handoff decision by allowing **mobile** station to synchronize with candidate **base station** for **identity**

verification , thus reducing the probability of a dropped call due to erroneous handoff decision...

...The figure shows flow chart of **mobile** assisted handoff method...
Title Terms: **MOBILE** ;
International Patent Class (Main): **H04Q-007/20**
Manual Codes (EPI/S-X): **W01-B05A1A** ...

... **W02-C03C1A** ...

... **W02-C03C1D** ...

... **W02-G03J1**

US006044272A

United States Patent [19]

Kobylinski et al.

[11] Patent Number: 6,044,272

[45] Date of Patent: Mar. 28, 2000

[54] **MOBILE ASSISTED HANDOFF SYSTEM AND METHOD**

[75] Inventors: **Richard A. Kobylinski; Milap V. Majmundar**, both of Austin, Tex.

[73] Assignee: **SBC Technology Resources, Inc.**, Austin, Tex.

[21] Appl. No.: **08/804,658**

[22] Filed: **Feb. 25, 1997**

[51] **Int. Cl.**[7] **H04Q 7/20**

[52] **U.S. Cl.** **455/437**; 455/436; 455/502; 370/331

[58] **Field of Search** 455/436, 437, 455/502, 503, 438, 439, 432, 450, 442; 370/331, 332

[56] **References Cited**

U.S. PATENT DOCUMENTS

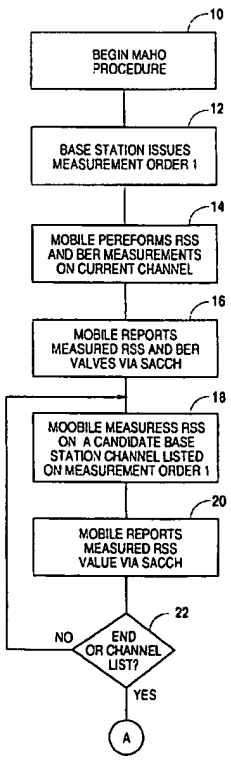
5,008,953	4/1991	Dahlin et al.	455/33
5,042,082	8/1991	Dahlin	455/33
5,157,661	10/1992	Kanai et al.	370/95.1
5,200,957	4/1993	Dahlin	370/100.1
5,228,029	7/1993	Kotzin	370/95.1
5,257,401	10/1993	Dahlin et al.	455/33.2
5,267,261	11/1993	Blakeney, II et al.	375/1
5,297,169	3/1994	Backstrom et al.	375/13
5,379,447	1/1995	Bonta et al.	455/437
5,381,443	1/1995	Borth et al.	375/1
5,410,733	4/1995	Niva et al.	455/33.2
5,428,816	6/1995	Barnett et al.	455/33.2
5,432,843	7/1995	Bonta	455/438
5,483,669	1/1996	Barnett et al.	455/33.2
5,493,563	2/1996	Rozanski et al.	370/50
5,517,673	5/1996	Febnel	455/33.1
5,517,674	5/1996	Rune	455/33.2
5,652,748	7/1997	Jolma et al.	455/436
5,722,073	2/1998	Wallstedt et al.	455/438
5,740,535	4/1998	Rune	455/437
5,778,075	7/1998	Haartsen	455/436

Primary Examiner—Dwayne D. Bost
Assistant Examiner—Nay A. Maune
Attorney, Agent, or Firm—Gunn, Lee & Keeling

[57] **ABSTRACT**

A system and method for improved mobile assisted handoff in a digital cellular communication system that gives the mobile station the ability to synchronize to candidate base station transmissions in order to read the transmitted digital voice color code (DVCC) of the candidate station. This process is performed during the idle period between two designated time slots in a TDMA frame. The invention is an enhancement to the existing mobile assisted handoff procedures described in the existing IS-136 standard. The present invention improves on the IS-136 standard's use of received signal strength measurements in that it allows the mobile station to acquire and report information regarding the digital verification color code (DVCC) of the candidate base station channels. Since the DVCC uniquely identifies the cell site to which a channel belongs, it is used to distinguish the candidate base station channel from its co-channel interferers, allowing the network to make a more informed handoff decision.

3 Claims, 3 Drawing Sheets



Memory Requirements:

681*2=1362 bits for Serial Correlation Method

1816*2=3632 bits for Parallel Correlation Method

It is worth noting, that the simulation results contained herein assume "rectangular" pulse shapes. In the actual IS-136 system, low pass filtering is employed in the transmitter as defined in the IS-136 standard. Filtering is also typically employed in the receiver. The effect of filtering is to degrade the performance from that predicted in FIGS. **5** and **6**, but the degree of degradation is expected to be negligible.

It is anticipated that these processing and memory requirements are either already within the limitations of existing digital cellular mobile stations or are within modifications easily implemented in existing mobile stations. The method of the present invention is, therefore, capable of implementation within the current confines of the IS-136 format and the technology associated with the tuning and data acquisition rates of existing mobile stations.

Although the present invention has been described in conjunction with a pre-defined format, it is anticipated that the steps involved in the present invention are applicable under a greater variety of conditions and formats than those described herein. The more specific scope of the present invention can best be identified by reference to the following claims.

We claim:

1. A method for mobile assisted handoff of a communication link between a mobile station and a base station in a digital cellular communications network, from a current base station to one of a number of candidate base stations within said network, said method comprising the steps of:

generating a list of a plurality of candidate channels for possible acceptance of said communication handoff;

transmitting a first measurement order from said current base station to said mobile station, said first measurement order containing said list of candidate channels;

measuring a received signal strength and a bit error rate at said mobile station for said communication between said mobile station and said current base station;

measuring received signal strength at said mobile station for each of said candidate channels listed in said first measurement order;

transmitting said received signal strength measurements from said mobile station to said current base station;

selecting a plurality of most favorable candidate channels from said received signal strength measurement results;

transmitting a second measurement order from said current base station to said mobile station, said second measurement order containing a list of said most favorable candidate channels;

tuning and synchronizing said mobile station to each of said candidate channels listed in said second measurement order, said step of tuning and synchronizing including:

tuning into said candidate channel, reading data within a time window on said candidate channel;

correlating said data from said candidate channel with a plurality of known synchronization words and identifying a most probable synchronization word within said data; and

returning back to said current base station channel;

reading and decoding an identification code for each of said candidate channels, said step of reading and decoding including:

storing said data from said candidate channel into a memory device located on said mobile station;

processing said data by searching for said identification code at a first predetermined number of symbols after the appearance of said probable synchronization word and, if said identification code cannot be found at said first predetermined number of symbols after said probable synchronization word, then searching for said identification code at a second predetermined number of symbols ahead of said probable synchronization word; and

identifying said identification code, said identification code comprising a digital voice color code word in said candidate channel;

transmitting said identification codes for each of said candidate channels from said mobile station to said current base station;

monitoring threshold received signal strength values for said current channel and said candidate channel, said threshold values determining when selection and activation of said handoff should occur; and

correlating said received signal strength measurements with said identification codes to identify an optimal candidate base station for effecting said handoff of said communication.

2. The method of claim **1** wherein said digital communication channels are formatted according to IS-136 standards for digital cellular radio communication and said candidate channel received signal strength measurements and said identification code readings are made by said mobile station during idle time slots within a frame.

3. An improved digital cellular communications system formatted according to IS-136 standards for digital cellular communication, the improvement comprising mobile station and base station elements for identifying candidate base stations for a communication handoff, making signal strength measurements on said candidate base stations, and selecting one of said candidate base stations to receive said communication handoff, said improved system comprising:

a current base station, said current base station being in communication on a current channel with a mobile station, said current base station having a memory for storing a first list of candidate base stations, said candidate base stations being those base stations proximate to said current base station and to which set communication handoff could occur;

a plurality of candidate base stations transmitting on a plurality of candidate channels, said transmissions containing synchronization and identification data;

a mobile station in communication with said current base station, said mobile station comprising:

means for making received signal strength measurements on said current channel and on said candidate channels;

means for tuning to said candidate channels and returning to said current channel;

means for synchronizing to said candidate channels including a data processing device and a memory device, said data processing device for correlating data on said candidate channel with known synchronization data and said memory device for storing said correlation and synchronization data, said data processing device and said memory device located on said mobile station, said data processing device

able to perform at least at a rate of a predetermined number of operations per measurement period and said memory device having at least a predetermined number of bits of memory;

means for readings said identification data on said candidate channels including said data processing device and said memory device, said data processing device for locating and decoding said identification data on said candidate channel and said memory device for storing said identification data; and

means for correlating said received signal strength measurements with said identification data and identifying from said correlation and optimal candidate base station to receive said communication handoff, said means for correlating said received signal strength measurements with said identification data comprises a data processing device located at said current base station.

* * * * *

31/3,K/33 (Item 33 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010456951 **Image available**
WPI Acc No: 1995-358270/199546
XRPX Acc No: N95-266273
Cellular mobile **phone user** identity verification - **using either memory or algorithm based verification before call is allowed from** particular **unit**
Patent Assignee: AT & T CORP (AMTT)
Inventor: WEN J C
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5457737	A	19951010	US 93174569	A	19931228	199546	B

Priority Applications (No Type Date): US 93174569 A 19931228
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5457737	A		13	H04Q-007/22	

Cellular mobile **phone user** identity verification - ...

...**using either memory or algorithm based verification before call is allowed from** particular **unit**

...Abstract (Basic): The automatic **identity verification** of a **mobile** phone user prior to connection of a requested call involves receiving a request by the **mobile** phone to the **base station** to connect a **wireless** call. A **unique** interrogation address is transmitted in response to the request a from the **base station** to the **mobile** phone. An expected code word is fetched from memory in the **base station** , the expected code word residing at the location **specified** by the **unique** interrogation address...

...A **unique** code word is retrieved from a memory within the **mobile** phone, the **unique** code word residing at the location **specified** by the **unique** interrogation address. The **unique** code word is transmitted from the **mobile** phone to the **base station** . It is verified that the expected code word fetched from the **base station** memory is the same as that received from the **mobile** phone. The requested **wireless** call is connected only when the code words are the same. The requested **wireless** call is denied when the code words are not the same...
Title Terms: **CELLULAR** ;
International Patent Class (Main): **H04Q-007/22**
International Patent Class (Additional): **H04M-011/00**
Manual Codes (EPI/S-X): **T01-J08C** ...

... **T01-S** ...

... **W01-C01D3A** ...

... **W01-C01D3D**

US005457737A

United States Patent [19]

Wen

[11] Patent Number: 5,457,737

[45] Date of Patent: Oct. 10, 1995

[54] **METHODS AND APPARATUS TO VERIFY THE IDENTITY OF A CELLULAR MOBILE PHONE**

[75] Inventor: **Jack C. Wen**, Parsippany, N.J.

[73] Assignee: **AT&T Corp.**, Murray Hill, N.J.

[21] Appl. No.: **174,569**

[22] Filed: **Dec. 28, 1993**

[51] **Int. Cl.**[6] **H04Q 7/22**; H04M 11/00

[52] **U.S. Cl.** **379/62**; 379/63; 379/58; 379/59; 455/53.1

[58] **Field of Search** 380/21, 23; 379/62, 379/59, 63, 58; 455/33.1, 54.1

[56] **References Cited**

U.S. PATENT DOCUMENTS

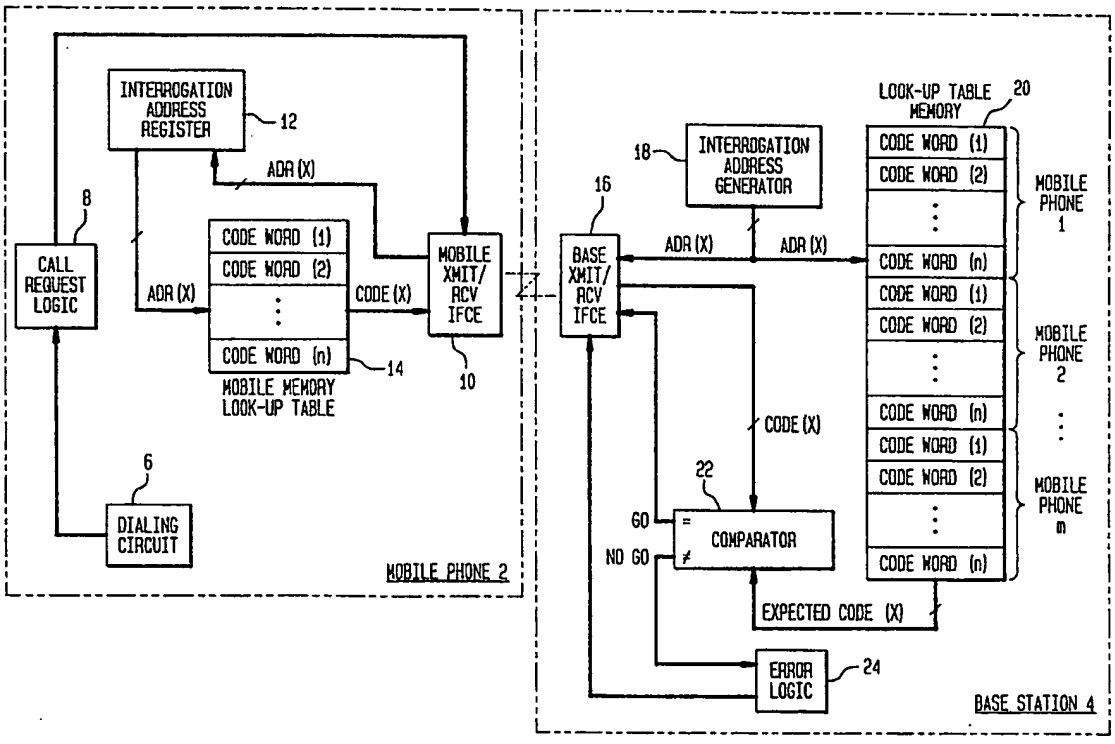
4,626,845	12/1986	Ley	380/23
4,955,049	9/1990	Ghisler	379/58
4,964,163	10/1990	Berry	380/23
5,077,790	12/1991	D'Amico et al.	379/62
5,091,942	2/1992	Dent	379/59
5,239,294	8/1993	Flanders et al.	379/63
5,293,576	3/1994	Mihm, Jr. et al.	380/21

Primary Examiner—Wing F. Chan
Assistant Examiner—William G. Trost

[57] **ABSTRACT**

A wireless-based communications system is provided with a method and apparatus for automatic verification of the identity of a mobile phone user in order to eliminate cellular piracy. A first embodiment implements a memory-based verification and a second embodiment implements an algorithm-based verification to reduce memory space requirements. The call is allowed when verification passes and is disallowed when verification fails.

30 Claims, 6 Drawing Sheets



phone calls directly to the user's mobile phone or landline phones, paging messages to the user's mobile phone (if equipped with this feature), or written notification (e.g. mail or fax). Additionally, every time a call passes initial verification, the system will interrupt the beginning of the call to play a short message indicating that there were multiple failed call attempts. This message would continue to play every time a call passes verification until ERRFLG is reset. If the legitimate user believes that illegitimate call attempts have been made, he/she can request a change in the PIN from the service provider. After the PIN has been changed, the error flag ERRFLG would then be reset. If the legitimate user does not suspect unauthorized use, ERRFLG would be reset and service would resume normally.

The error routine of FIG. **5** is implemented by the error logic **24** by using any means known in the art for accomplishing the required functions (e.g. counting means, comparator means and the like).

For privacy and security applications, the code words can also be used to scramble voice and data during calls.

Although the methods and apparatus of the present invention has been described with reference to the verification of a mobile phone in a cellular phone system, such methods and apparatus can also be used in new emerging wireless systems such as the Personal Communications Services (PCS) and wireless LAN applications. In addition, said verification system can be implemented in any wireless communications system which may be susceptible to piracy by illegitimate users.

I claim:

1. A method for a base station in a wireless-based communications system to automatically verify the identity of a mobile phone prior to connecting a requested wireless call, the method comprising the steps of:

(a) receiving a request by the mobile phone to the base station to connect a wireless call;

(b) transmitting in response to the request a unique interrogation address from the base station to the mobile phone;

(c) fetching from memory in the base station an expected code word, the expected code word residing at the location specified by the unique interrogation address;

(d) fetching from memory in the mobile phone a unique code word, the unique code word residing at the location specified by the unique interrogation address;

(e) transmitting the unique code word from the mobile phone to the base station;

(f) verifying that the expected code word fetched from the base station memory is the same as the unique code word received from the mobile phone;

(g) connecting the requested wireless call only when the code words are the same; and

(h) denying the requested wireless call when the code words are not the same.

2. The method of claim **1** comprising the additional step of

(i) changing the unique interrogation address prior to a subsequent verification whereby the unique code word fetched from the mobile phone memory and the expected code word fetched from the base station memory are different from prior verifications.

3. The method of claim **2** in which the interrogation address changing step is effected incrementally.

4. The method of claim **2** in which the interrogation address changing step is effected pseudo-randomly.

5. The method of claim **2** comprising the additional step of:

(j) informing the mobile phone that the requested wireless call has been denied.

6. The method of claim **5** comprising the additional steps of:

(k) counting the number of failed verifications within a preset time period; and

(l) alerting the service provider when the number of failed verifications within a preset time period is more than a preset amount.

7. In a wireless-based communications system having a base station and at least one mobile phone, apparatus for automatically verifying the identity of a mobile phone prior to connecting a requested wireless call comprising:

(a) means in the mobile phone to request the connection of a wireless call:

(b) means in the base station to generate and transmit a unique interrogation address in response to the mobile phone request;

(c) memory means in the base station for storing a set of expected unique code words reserved for each mobile phone in the wireless-based system;

(d) memory means in the mobile phone for storing a set of unique code words identical to the set reserved in the base station memory means for the particular mobile phone;

(e) means to provide to the base station the unique code word from the mobile phone memory means which corresponds to the unique interrogation address;

(f) means in the base station to compare the mobile phone code word with the expected code word from the base station memory means which corresponds to the unique interrogation address; and

(g) means for connecting the wireless call only when the mobile phone code word is the same as the base station expected code word and for denying the connection of the wireless call when the mobile phone code word and is not the same as the base station expected code word.

8. The wireless-based communications system of claim **7** further comprising:

(h) means for changing the unique interrogation address prior to a subsequent verification whereby the unique code word from the mobile phone memory means and the expected code word from the base station memory are changed from prior verifications.

9. The wireless-based communications system of claim **8** in which the address changing means is an incremental counter.

10. The wireless-based communications system of claim **8** in which the address changing means is a pseudo-random number generator.

11. The wireless-based communications system of claim **8** further comprising:

(i) means for informing the mobile phone that the requested wireless call has been denied.

12. The wireless-based communications system of claim **11** further comprising:

(j) means for counting the number of failed verifications within a preset time period; and

(k) means for alerting the service provider when the number of failed verifications within a preset time period is more than a preset amount.

13. In a wireless-based communications system comprising a plurality of mobile phones and a base station capable

of communicating with each of the mobile phones, a system for verifying the identity of any of the mobile phones wherein:

(a) each of the mobile phones comprises:

(i) means to request the connection of a wireless call,

(ii) means to receive a unique interrogation address provided by the base station in response to the request,

(iii) memory means for storing a set of predetermined unique code words, and

(iv) means to provide to the base station a unique mobile phone code word from the memory means which corresponds to the unique interrogation address, and

(b) the base station comprises:

(i) means to provide a unique interrogation address to a mobile phone in response to a request by the mobile phone to establish a wireless call,

(ii) means to receive a unique mobile phone code word provided by the mobile phone in response to the unique interrogation address,

(iii) memory means for storing a plurality of sets of unique expected code words, wherein each set of expected code words is identical to a set of unique code words stored in memory means in each mobile phone,

(iv) means to compare the expected code word corresponding to the interrogation address with the received unique mobile phone code word, and

(v) means to allow the connection of a wireless call only when the unique mobile phone code word is the same as the expected code word and for disallowing the connection of a wireless call when the unique mobil phone code word and is not the same as the expected code word.

14. The wireless-based communications system of claim **13** wherein the base station further comprises:

(b)(vi) means for changing the unique interrogation address prior to a subsequent verification whereby the unique code word from the mobile phone memory means and the expected code word from the base station memory are changed from prior verifications.

15. The wireless-based communications system of claim **14** in which the address changing means is an incremental counter.

16. The wireless-based communications system of claim **14** in which the address changing means is a pseudo-random number generator.

17. The wireless-based communications system of claim **14** wherein the base station further comprises:

(b)(vii) means for informing the mobile phone that the requested wireless call has been denied.

18. The wireless-based communications system of claim **17** wherein the base station further comprises:

(b)(viii) means for counting the number of failed verifications within a preset time period; and

(b)(ix) means for alerting the service provider when the number of failed verifications within a preset time period is more than a preset amount.

19. A method for a base station in a wireless telephone system to automatically verify the identity of a mobile phone prior to connecting the mobile phone with a dialed phone, the method comprising the steps of:

(a) receiving a request by the mobile phone to the base station to connect with the dialed phone;

(b) providing to the base station from the mobile phone a mobile phone number dedicated to the mobile phone for identifying to the base station the particular mobile phone requesting the phone call;

(c) fetching from memory in the base station an expected PIN and an expected electronic serial number corresponding to the received mobile phone number;

(d) transmitting a unique interrogation address from the base station to the mobile phone;

(e) implementing in the base station a predetermined algorithm to generate an expected code word as a function of the unique interrogation address and the expected PIN;

(f) implementing in the mobile phone the predetermined algorithm to generate a code word as a function of the unique interrogation address and the mobile phone PIN;

(g) encrypting in the mobile phone a first message as a function of the electronic serial number and the generated code word and a second message as a function of the dialed phone number and the generated code word;

(h) transmitting the first and second encrypted messages to the base station;

(i) deciphering in the base station the received messages by using the expected code word to obtain a deciphered electronic serial number and a deciphered dialed phone number;

(j) verifying that the expected mobile phone number fetched from the base station memory is the same as the deciphered electronic serial number;

(k) connecting the wireless call with the deciphered dialed phone number only when verification passes; and

(l) disallowing the phone call when the verification fails.

20. The method of claim **19** comprising the additional step of:

(m) changing the unique interrogation address prior to a subsequent verification whereby the unique code word generated by the algorithm in the mobile phone and the expected code word generated by the algorithm in the base station are different from prior verifications.

21. The method of claim **20** in which the interrogation address changing step is effected incrementally.

22. The method of claim **21** in which the interrogation address changing step is effected pseudo-randomly.

23. The method of claim **20** comprising the additional step of:

(n) informing the mobile phone that the requested wireless call has been denied.

24. The method of claim **23** comprising the additional steps of:

(o) counting the number of failed verifications within a preset time period; and

(p) alerting the service provider when the number of failed verifications within a preset time period is more than a preset amount.

25. In a wireless-based communications system having a base station and at least one mobile phone, apparatus for automatically verifying the identity of a mobile phone prior to connecting a requested wireless call comprising:

(a) means in the mobile phone to request the connection of a wireless call:

(b) means in the mobile phone to provide to the base station a mobile phone number dedicated to the mobile phone for identification of the particular mobile phone requesting the call;

(c) memory means in the base station for storing an expected PIN and an expected electronic serial number corresponding to the mobile phone number for each mobile phone in the system;

(d) means in the base station to generate and transmit a unique interrogation address in response to the mobile phone request;

(e) means in the base station to implement a predetermined algorithm to generate an expected code word as a function of the unique interrogation address and the expected PIN corresponding to the mobile phone number received from the mobile phone;

(f) means in the mobile phone to implement the predetermined algorithm to generate a code word as a function of the unique interrogation address received from the base station and of the mobile phone's PIN;

(g) means in the mobile phone to encrypt a first message as a function of the electronic serial number and the generated code word and a second message as a function of the dialed phone number and the generated code word;

(h) means to transmit the first and second encrypted messages to the base station;

(i) means in the base station to decipher the received encrypted messages by using the expected code word to obtain a deciphered electronic serial number and a deciphered dialed phone number;

(j) means in the base station to verify that the expected electronic serial number fetched from the base station memory is the same as the deciphered electronic serial number;

(k) means in the base station to connect the wireless call with the deciphered dialed phone number only when verification passes and to disallow the wireless call when the verification fails.

26. The wireless-based communications system of claim **25** further comprising:

(l) means for changing the unique interrogation address prior to a subsequent verification whereby the unique code word generated by the algorithm in the mobile phone and the expected code word generated by the algorithm in the base station are different from prior verifications.

27. The wireless-based communications system of claim **26** in which the address changing means is an incremental counter.

28. The wireless-based communications system of claim **26** in which the address changing means is a pseudo-random number generator.

29. The wireless-based communications system of claim **26** further comprising:

(m) means for informing the mobile phone that the requested wireless call has been denied.

30. The wireless-based communications system of claim **29** further comprising:

(n) means for counting the number of failed verifications within a preset time period; and

(o) means for alerting the service provider when the number of failed verifications within a preset time period is more than a preset amount.

* * * * *

31/3,K/35 (Item 35 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010211741 **Image available**
WPI Acc No: 1995-112995/ **199515**
XRPX Acc No: N96-109020
Subscriber registration system for cordless telephone unit - involves base and substations linked by radio **with controller and memories for storing equipment identification code and entry of subscriber equipment data**
Patent Assignee: NEC CORP (NIDE)
Inventor: KOJIMA S
Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 7038955	A	19950207	JP 93155518	A	19930625	199515	B
US 5495520	A	19960227	US 94264057	A	19940622	199614	

Priority Applications (No Type Date): JP 93155518 A 19930625
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 7038955	A		17	H04Q-007/38	
US 5495520	A		15	H04Q-007/20	

... **involves base and substations linked by** radio **with controller and memories for storing equipment identification code and entry of subscriber equipment data**

...Abstract (Basic): The system consists of two or **more base stations** (101, 102) linked by **radio** to substations (201, **202**). It is **provided** with transmitting and receiving circuits (12, 22) controllers (14, **24**), **base stations** identification code memory units (15, 25) **and** substations identification code memory units (16, 26). The **base station** operating part (17) in the **base station** and the sub station **operating** part (27) in the sub stations facilitate the registration of a subscriber in the system...

... In order to **set** up a new connection for a subscriber, the **subscribers** sub stations **identification** code, **the** sub stations password and the password of the local **base station** are entered into the **base station** operating parts. Similarly, into the sub station operation part, the above information are entered. This...

...the sub station password in the memory. When there is conformity, the controller stores the **base station** equipment identification code in memory. A registration completion signal comprising of the subscribers **base station identification** code, **base station password** and the concerned sub station equipment identification code is then transmitted from the sub stations. The **base station** receives this signal and received **base station** password is matched with the contents in memory. When a match is found, the **sub** station equipment **identification** code is stored in memory...

...includes a number of groups of master units and slave units for being connected to **each** other, and **each** including transmitting/receiving device for interchanging signals over a **radio** channel. The master units and the slave units **each** includes a storing device for storing a master unit ID code and a slave unit ID code which are different from **each** other...

...A control device of **each** master unit includes a device for transmitting a registration signal to which are added slave unit ID codes and slave unit password stored in master unit. **Each** control unit of the slave units includes a device for storing ID code and slave

...Title Terms: **ASSIGN** ;

International Patent Class (Main): **H04Q-007/20** ...

... **H04Q-007/38**

International Patent Class (Additional): **H04M-001/00**

Manual Codes (EPI/S-X): **W01-C01D1D**

US005495520A

United States Patent [19]

Kojima

[11] Patent Number: 5,495,520

[45] Date of Patent: Feb. 27, 1996

[54] **CORDLESS TELEPHONE SYSTEM AND IDENTIFICATION CODE SETTING METHOD THEREFOR**

[75] Inventor: **Susumu Kojima**, Tokyo, Japan

[73] Assignee: **NEC Corporation**, Tokyo, Japan

[21] Appl. No.: **264,057**

[22] Filed: **Jun. 22, 1994**

[30] **Foreign Application Priority Data**

Jun. 25, 1993 [JP] Japan 5-155518

[51] **Int. Cl.**[6] **H04Q 7/20**

[52] **U.S. Cl.** **379/62**; 379/61

[58] **Field of Search** 379/62, 61, 63, 379/58, 356, 354, 355

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,979,205	12/1990	Haraguchi et al.	379/61
5,068,889	11/1991	Yamashita	379/62
5,157,710	10/1992	Itoh	379/62

FOREIGN PATENT DOCUMENTS

2309847 12/1990 Japan .

Primary Examiner—Curtis Kuntz
Assistant Examiner—Michael B. Chernoff
Attorney, Agent, or Firm—Whitham, Curtis, Whitham & McGinn

[57] **ABSTRACT**

In a cordless telephone system, a master unit adds to a registration signal an identification (ID) code assigned to a slave unit connectable to the master unit, a master unit transmission password, and an ID code assigned to the master unit, and sends the resulting registration signal to the slave unit. On receiving the registration signal, the slave unit determines whether or not the master unit transmission password is identical with a slave unit password stored therein. If the former is identical with the latter, the slave unit writes the master unit ID code therein, adds the master unit ID code, slave unit transmission password, and slave unit ID code to an end-of-registration signal, and then sends the signal to the master unit. On receiving the end-of-registration signal, the master unit writes the slave unit ID code included in the signal if the slave unit transmission password is identical with a password stored therein.

7 Claims, 8 Drawing Sheets

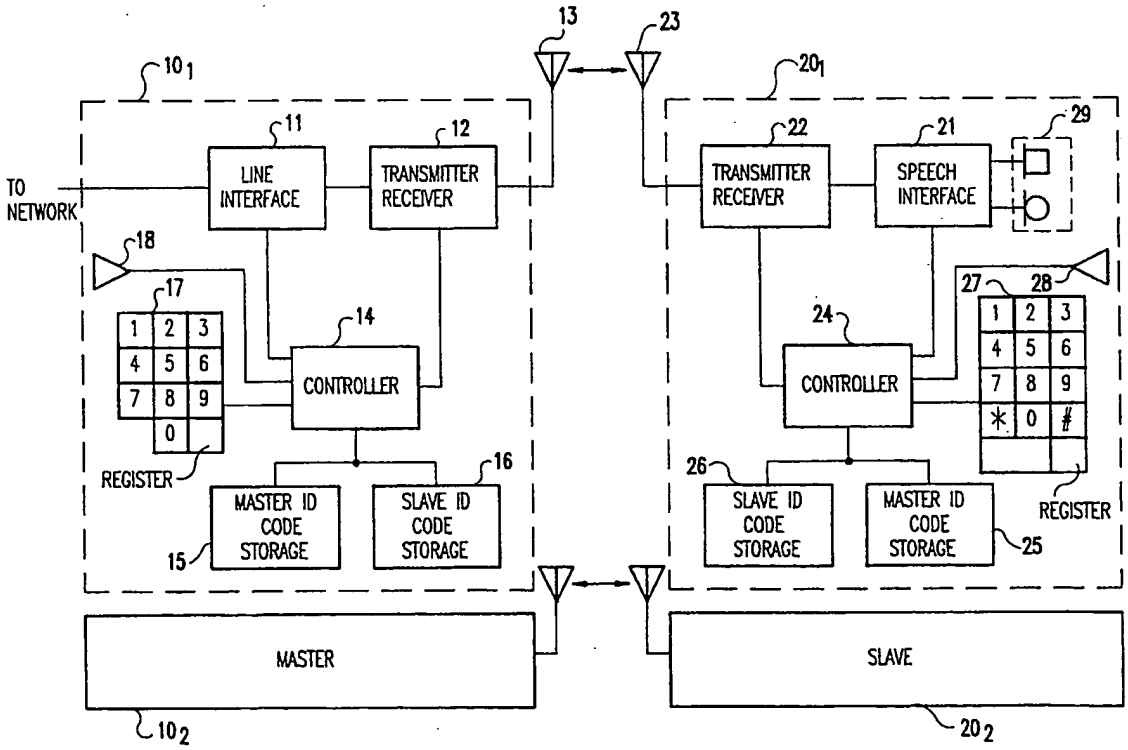


FIG. **1**. The master unit executes the procedure shown in FIG. **5**.

FIG. **8** schematically shows a cordless telephone system representative of a fifth embodiment of the present invention. As shown, the system includes a main unit **30**, a plurality of master units **36**, and a plurality of slave units, not shown. The main unit **30** has a line interface switch **31**, a controller **32**, an operating section **33**, and a slave unit ID code storage **34**. This embodiment is similar to the first embodiment except that the main unit **30** is provided witch the slave unit ID code storage **34** and the operating section **33**. The system of FIG. **8** is, in principle, operated in the same manner as the system of FIG. **1** except that the main unit **30** and master units **36** cooperate as if they were the master unit **10**, FIG. **1**.

In summary, it will be seen that the present invention provides a cordless telephone system which eliminates erroneous connection even when a plurality of pairs of master and slave units adjoining each other are operated for registration at the same time, thereby promoting sure registration. In addition, the system ensures safe registration even if the ID codes of the units are known to a third party.

Various modifications will become possible for those skilled in the art after receiving the teachings of the present disclosure without departing from the scope thereof. For example, in the first, second and fifth embodiments, the slave unit stores, on receiving a correct registration signal from the master unit (main unit), a master unit ID code without volatilizing it. Alternatively, in a surer and safer procedure, the master unit (main unit) may send, on receiving an end-of-registration signal from the slave unit, an acknowledge signal to the slave unit and store a slave unit ID signal in a nonvolatile manner, in which case the slave unit will store the master unit ID code in a nonvolatile manner in response to the acknowledge signal. In the third and fourth embodiments, the master unit stores, on receiving a correct registration signal from the slave unit, a slave unit ID code without volatilizing it. These embodiments may be modified, for a sureness and safety purpose, such that the slave unit sends, on receiving an end-of-registration signal from the master unit, an acknowledge signal to the master unit and stores a master unit ID signal in a nonvolatile fashion, while the master unit stores a slave unit ID code in response to the acknowledge signal.

The illustrative embodiments are arranged such that the slave unit ID code storage **16** of the master unit **10**, or the storage **34** of the main unit **30**, and the master unit ID code storage **25** of the slave unit **20** are each caused to write the ID code of the slave unit or that of the master unit in an idle address location thereof. If desired, the user may enter an address location number together with the other information in the event of registration. This makes it possible to replace an ID code registered at a certain address location of the storage **16** or **34** with an ID code assigned to a new unit or to cancel the registration in the storage **16** or **34**. Furthermore, when a particular extension number is given to each slave unit, as in a PBX (Private Branch Exchange), the storages **16** and **34** may have the address locations thereof managed on an extension number basis; then the user will enter an address location number in the form of an extension number.

What is claimed is:

1. A cordless telephone system comprising:

a plurality of groups of master units and slave units for being connected to each other, and each including transmitting/receiving means for interchanging signals over a radio channel,

said master units and said slave units each comprising storing means for storing a master unit ID code and a slave unit ID code which are different from each other, and control means for controlling said transmitting/receiving means,

said master units each comprising master unit operating means accessible for entering the slave unit ID code and a slave unit password assigned to one of said slave units to be newly connected to the master unit, and a master unit password assigned to said master unit,

said slave units each comprising slave unit operating means accessible for entering the master unit ID code and the master unit password assigned to said master unit to which said slave unit is to be newly connected, and the slave unit password assigned to said slave unit,

said control means of said master units each comprising means for transmitting a registration signal to which are added the slave unit ID code and slave unit password having been entered, and the master unit ID code stored in said master unit;

said control means of said slave units each comprising means for storing, if the slave unit ID code and the slave unit password added to the registration signal are respectively identical with the slave unit ID code stored and the slave unit password entered, said slave unit ID code of said registration signal in said storing means, and sending an end-of-registration signal to which are added the master unit ID code added to said registration signal, the master unit entered, and said slave unit ID code stored,

said control means of said master units each further comprising means for storing, if the master unit ID code and the master unit password added to the end-of-registration signal are respectively identical with the master unit ID code stored and the master unit password entered, the slave unit ID code having been added to said end-of-registration signal.

2. A system as claimed in claim **1**, wherein said control means of said master unit and said slave unit, which are for being connected to each other, respectively further comprise means for adding the master unit ID code and the slave unit ID code stored to control signals to be interchanged, to thereby confirm a unit sent said control signals and a unit to receive said control signals, whereby erroneous connection is eliminated.

3. A cordless telephone system comprising:

a plurality of groups of master units and slave units for being connected to each other, and each including transmitting/receiving means for interchanging signals over a radio channel,

said master units and said slave units each comprising storing means for storing a master unit ID code arid a slave unit ID code which are different from each other, and control means for controlling said transmitting/receiving means,

said master units each comprising master unit operating means accessible for entering the slave unit ID code and a slave unit password assigned to one of said slave units to be newly connected to the master unit, and a master unit password assigned to said master unit,

said slave units each comprising slave unit operating means accessible for entering a master unit password assigned to the master unit to which the slave unit is to be newly connected, and the slave unit password assigned to said slave unit,

said control means of said master units each comprising means for transmitting a registration signal to which are

added the slave unit ID code and the slave unit password entered, and the master unit ID code stored,

said control means of said slave units each comprising means for storing, if the slave unit ID code and the slave unit password added to the registration signal are respectively identical with the slave unit ID code stored and the slave unit password entered, said slave unit ID code of said registration signal in said storing means, and sending an end-of-registration signal to which are added the master unit ID code added to said registration signal, the master unit password entered, and said slave unit ID code stored,

said control means of said master units each further comprising means for storing, if the master unit ID code and the master unit password added to the end-of-registration signal are respectively identical with the master unit ID code stored and the master unit password entered, the slave unit ID code having been added to said end-of-registration signal.

4. A cordless telephone system comprising:

a plurality of groups of master units and slave units for being connected to each other, and each including transmitting/receiving means for interchanging signals over a radio channel,

said master units and said slave units each comprising storing means for storing a master unit ID code and a slave unit ID code which are different from each other, and control means for controlling said transmitting/receiving means,

said slave units each comprising slave unit operating means accessible for entering the master unit ID code and a master unit password assigned to said master unit to which the slave unit is to be newly connected, and said slave unit password assigned to said slave unit,

said master units each comprising master unit operating means accessible for entering the slave unit ID code and a slave unit password assigned to one of said slave units to be newly connected to the master unit, and a master unit password assigned to said master unit,

said control means of said slave units each comprising means for transmitting a registration signal to which are added the master unit ID code and the slave unit password entered, and the slave unit ID code assigned to the slave unit,

said control means of said master units each comprising means for storing, if the master unit ID code and the master unit password added to the registration signal are respectively identical with the master unit ID code stored and the master unit password entered, the slave unit ID code of said registration signal in said storing means, and sending an end-of-registration signal to which are added said slave unit ID code and the slave unit password entered, and said master unit ID code stored,

said control means of said slave units each further comprising means for storing, if the slave unit ID code and the slave unit password added to the end-of-registration signal are respectively identical with the slave unit ID code stored and the slave unit password entered, the master unit ID code having been added to said end-of-registration signal.

5. A cordless telephone system comprising:

a plurality of master units and a plurality of slave units for being connected to each other, and each including transmitting/receiving means for interchanging signals over a radio channel,

said master units and said slave units each comprising storing means for storing a master unit ID code and a slave unit ID code which are different from each other, and control means for controlling said transmitting/receiving means,

said slave units each comprising slave unit operating means accessible for entering the master unit ID code and a master unit password assigned to the master unit to which the slave unit is to be newly connected, and a slave unit password assigned to said slave unit,

said master units each comprising master unit operating means accessible for entering the slave unit ID code assigned to the slave unit which is to be newly connected to the master unit, and a master unit password assigned to said master unit,

said control means of said slave units each comprising means for transmitting a registration signal to which are added the master unit ID code entered and the master unit password entered, and the slave unit ID code stored,

said control means of said master units each comprising means for storing, if the master unit ID code and the master unit password added to the registration signal are respectively identical with the master unit ID code stored and the master unit password entered, the slave unit ID code of said registration signal in said storing means, and sending an end-of-registration signal to which are added the slave unit ID code added to said registration signal, the slave unit password entered, and said master unit ID code stored,

said control means of said slave units each further comprising means for storing, if the slave unit ID code and the slave unit password added to the end-of-registration signal are respectively identical with the slave unit ID code stored and the slave unit password entered, the master unit ID code having been added to said end-of-registration signal.

6. A cordless telephone system comprising:

a plurality of groups of master units and slave units for being connected to each other and each including transmitting/receiving means for interchanging signals over a radio channel and transmission/reception control means for controlling said transmitting/receiving means, and a main unit including a line interface switch connected to said master units by respective wired channels and switch control means for controlling said line interface switch,

said slave units each comprising slave unit storing means for storing a master unit ID code assigned to the master unit, to which the slave unit is connectable, and a slave unit ID code of said slave unit which is different from said master unit ID code,

said main unit comprising main unit storing means for storing the slave unit ID code of the slave unit connectable to the master unit,

said master units each comprising master unit storing means for storing the master unit ID code assigned thereto,

said main unit comprising main unit operating means accessible for entering the slave unit ID code and a slave unit password assigned to one of said slave units to be newly connected, and a main unit password,

said switch control means comprising means for outputting a registration signal to which are added the slave unit ID code and the slave unit password entered,

said transmission/reception control means of said master units each comprising means for transmitting the registration signal by adding the master unit ID code stored,

said slave units each comprising slave unit operating means accessible for entering the master unit ID code assigned to the master unit to which the slave unit is to be newly connected, a main unit password, and the slave unit password assigned to said slave unit,

said transmission/reception control means of said slave units each comprising means for storing, if the slave unit ID code and the slave unit password added to the registration signal are respectively identical with the slave unit ID code stored and the slave unit password entered, the master unit ID code of said registration signal in said storing means, and means for sending an end-of-registration signal to which are added said master unit ID code and the main unit password entered, and the slave unit ID code stored,

said transmission/reception control means of said master units each further comprising means for receiving the end-of-registration signal including the master unit ID code stored,

said switch control means further comprising means for storing, if the main unit password added to the end-of-registration signal received is identical with the main unit password entered, the slave unit ID code having been added to said end-of-registration signal.

7. A system as claimed in claim **6**, wherein said switch control means, said transmission/reception control means of said master units, and said transmission/reception control means of said slave units further comprise means for adding the master unit ID code and the slave unit ID code stored to control signals to be interchanged, to thereby confirm a unit sent said control signals and a unit to receive said control signals, whereby erroneous connection is eliminated.

* * * * *

31/3,K/11 (Item 11 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013773140 **Image available**
WPI Acc No: 2001-257351/200126
XRPX Acc No: N01-183583
Uplink detection of scheduled mobile **involves reserving resource for transmission regardless of whether packet has been correctly received, once identity of** mobile **station has been verified**
Patent Assignee: TELEFONAKTIEBOLAGET ERICSSON L M (TELF)
Inventor: LINDSKOG J; POHJANVUORI T; RYDNELL G
Number of Countries: 095 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200103452	A1	20010111	WO 2000SE1357	A	20000627	200126	B
AU 200060376	A	20010122	AU 200060376	A	20000627	200130	
EP 1197102	A1	20020417	EP 2000946650	A	20000627	200233	
			WO 2000SE1357	A	20000627		
KR 2002016842	A	20020306	KR 2001716549	A	20011224	200261	
CN 1359596	A	20020717	CN 2000809868	A	20000627	200268	
JP 2003503982	W	20030128	WO 2000SE1357	A	20000627	200309	
			JP 2001508182	A	20000627		
US 6519469	B1	20030211	US 99347022	A	19990702	200314	
CN 1134186	C	20040107	CN 2000809868	A	20000627	200570	

Priority Applications (No Type Date): US 99347022 A 19990702
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200103452	A1	E	27	H04Q-007/22	
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW					
AU 200060376	A			H04Q-007/22	Based on patent WO 200103452
EP 1197102	A1	E		H04Q-007/22	Based on patent WO 200103452
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
KR 2002016842	A			H04L-012/56	
CN 1359596	A			H04Q-007/22	
JP 2003503982	W		29	H04L-012/28	Based on patent WO 200103452
US 6519469	B1			H04B-007/00	
CN 1134186	C			H04Q-007/22	

Uplink detection of scheduled mobile **involves reserving resource for transmission regardless of whether packet has been correctly received, once identity of** mobile **station has been verified**

Abstract (Basic):
... A **base station** reserves a resource for transmission of at least **one** subsequent packet from a **mobile** station regardless of whether a packet has been correctly received from the **mobile** station, if the correlation between stored data and the packet **verifies** the **identity** of the **mobile** station.
... The method starts with the **base station** storing data associated with the **mobile** station from a first packet data transaction. The **base station** then determines if the packet from the **mobile** station for starting a second packet data transaction has been correctly received. The stored data are correlated with the

packet. **INDEPENDENT** CLAIMS are also included for the following...

...b) and a **base station** .
...

...For **radio** communication system...

...Minimizes battery consumption by **mobile** station during real-time applications while minimizing delay response times...
...The figure illustrates a state diagram for a **mobile** station
...Title Terms: **SCHEDULE** ;
...International Patent Class (Main): **H04L-012/28** ...

... **H04L-012/56** ...

... **H04Q-007/22**
International Patent Class (Additional): **H04Q-007/38**
Manual Codes (EPI/S-X): **W01-B05A1A** ...

... **W02-C03C1D**

US006519469B1

(12) **United States Patent**
Rydnell et al.

(10) **Patent No.: US 6,519,469 B1**
(45) **Date of Patent: Feb. 11, 2003**

(54) **UPLINK DETECTION OF SCHEDULE MOBILES FOR AVOIDING ACCESS DELAYS**

(75) Inventors: **Gunnar Rydnell**, Rävlanda (SE); **Jan Lindskog**, Pixbo (SE); **Timo Pohjanvuori**, Göteborg (SE)

(73) Assignee: **Telefonaktiebolaget LM Ericsson (publ)**, Stockholm (SE)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/347,022**

(22) Filed: **Jul. 2, 1999**

(51) **Int. Cl.**[7] **H04B 7/00**
(52) **U.S. Cl.** **455/466**; 370/349
(58) **Field of Search** 370/348, 349, 370/355, 352, 311; 455/466, 455, 450, 452, 574

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,539,748 A		7/1996	Raith	
5,673,259 A		9/1997	Quick, Jr.	
5,708,656 A		1/1998	Noneman et al.	
5,802,465 A	*	9/1998	Hamalainen et al.	455/403
6,249,681 B1	*	6/2001	Virtanen	370/349

FOREIGN PATENT DOCUMENTS

EP	0681406 A1 *	8/1995	H04Q/7/24
EP	0 681 406	11/1995	
EP	0872982 A1	10/1998	
WO	WO97/37504	10/1997	

* cited by examiner

Primary Examiner—Thanh Cong Le
Assistant Examiner—Nick Corsaro

(57) **ABSTRACT**

The present invention provides a method and system for reducing the delay of the transmission of packet data including storing, by a base station, data associated with a mobile station from a first packet data transaction. A packet for starting a second packet data transaction is received from a mobile station and the base station determines whether or not the packet has been correctly received. The base station correlates at least one field in the packet with the stored data. If the base station is able to identify the mobile station based on the correlation with the stored data, then the base station reserves a resource for transmission of a subsequent packet from the mobile station regardless of whether or not the packet has been correctly received.

21 Claims, 7 Drawing Sheets

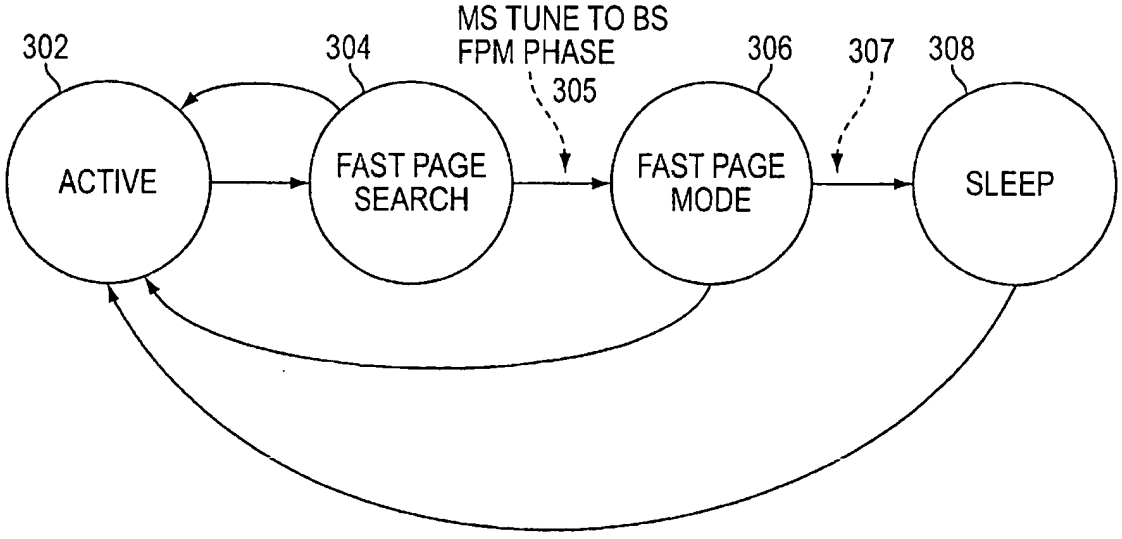


FIG. **5** illustrates an exemplary signal diagram between the base station and the mobile station operating in FPM. The base station (BS) has reserved predetermined uplink and downlink time slots for the mobile station (MS) as transmission opportunities with a predetermined periodicity. When the mobile station has uplink data to send to the base station, it sends, at its scheduled uplink time slot, a signal **550** containing packet **430** (see FIG. **4**) indicating in the PDU type field **432** that the packet is a Begin frame. The base station uses the value of the CRC field **442** to verify the information in the packet.

If the base station cannot verify the information in the packet, the base station sends a non-acknowledgment message **552** to the mobile station. At the next scheduled opportunity in FPM, the mobile station will retransmit **554** the packet **430**. If, after retransmission the packet is verified, then the base station returns an acknowledgment message **556**, receives the first data field **440**, and receives the remaining packets in active mode (illustrated as signal **558**).

A decay in the QoS of a communication may occur in the case where the mobile station must wait until the next scheduled opportunity to retransmit its Begin frame. However, in an alternate embodiment of the present invention, this potential decay can be mitigated by taking advantage of the structure of the packet **430**. For example, for a given mobile station, at least one of, and possibly all of the MSID field **434**, mobile station capability field **436**, and modulation proposal field **438** have the same value for each packet sent by the same mobile station.

The base station therefore, can store these known values from an earlier communication (a previous active mode communication or a request from the mobile station to enter FPM) with the mobile station in order to anticipate the above-mentioned fields for future communications. In addition, if the base station is anticipating a Begin frame from the mobile station (e.g., during FPM), then when the mobile station sends the Begin frame, the PDU type field **432** is also known by the base station.

The present invention takes advantage of the base station's ability to anticipate the values of the fields which precede the data field **440** so that the base station can correlate the received known packet field values with stored values from a previous communication with the mobile station. In this way, even if the CRC fails and the data cannot be reliably decoded, if the base station was able to correlate the values received in one or more of, for example, fields **432, 434, 436** and **438** from a previous transaction, then the base station would know that the specific mobile station attempted to establish a MAC transaction. One skilled in the art will recognize that the base station can correlate to any combination or portion of the fields **432–438** to identify the packet's originator. However, the accuracy of the correlation will be dependent on the number of bits correlated.

An exemplary method of correlating the packet fields is to perform a bit by bit comparison of the received data. If a predetermined number of bits match, then the base station can assume that the two packet fields match. One skilled in the art will recognize that the percentage of bits required for a match is dependent on the desired tolerance of the system which may, for example, be based on the total number of mobile stations and/or the length of the packet fields.

FIG. **6** illustrates an exemplary signal diagram between a base station and a mobile station applying the above technique. The base station (BS) has reserved predetermined uplink and downlink time slots for the mobile station (MS) as transmission opportunities with a predetermined periodicity. When the mobile station has uplink data to send to the base station, it sends at its scheduled uplink time slot, a signal **650** containing packet **430** (see FIG. **4**) indicating in the PDU type field **432** that the packet is a Begin frame. The base station uses the value of the CRC frame **442** to verify the information in the packet.

In an exemplary embodiment of the present invention, if the base station cannot verify the information in the packet, the base station sends a non-acknowledgment message **652** to the mobile station. However, in this case, since the base station has reserved this opportunity for the mobile station, it assumes that the communication received, even if it the data cannot be decoded, is from the mobile station. The base station then attempts to correlate the stored values of the MSID, PDU Type, MS Capability, and Modulation Proposal frames **(432–438)** with the received values from the signal **650**. If the base station is able to correlate the above values, then the base station schedules the mobile station to retransmit the data in active mode, rather than waiting to receive another Begin frame in FPM. Allowing the mobile station to enter active mode without having to wait for the next reserved time slot in FPM reduces the delay for the transmission of the packet, thereby providing a higher QoS. The mobile station resends the Begin frame signal **650** at the newly scheduled time slot and the base station acknowledges the receipt of the signal with an acknowledgment signal **654**. The remaining packets are subsequently sent and acknowledged (represented by signals **660** and **654**, respectively) in active mode.

In an alternate embodiment of the present invention, the mobile station sends the Begin frame in response to a signal from the base station including the mobile station identification number indicating the occurrence of an uplink scheduling opportunity for the mobile station. Furthermore, while the above-described embodiments were provided using FPM as an exemplary protocol for the present invention, one skilled in the art will appreciate that the present invention may be practiced under numerous wireless communication protocols. For example, the signal from the base station may be sent to the mobile station while the mobile station is in active mode, FPM, or sleep mode.

The foregoing has described the principles, preferred embodiments and modes of operation of the present invention. However, the invention should not be construed as being limited to the particular embodiments discussed above. While the above-described embodiments were provided using TDMA, one skilled in the art will appreciate that the present invention may be practiced in any of a number of different protocols such as CDMA, FDMA, TDD, etc. Thus, the above-described embodiments should be regarded as illustrative rather than restrictive, and it should be appreciated that variations may be made in those embodiments by workers skilled in the art without departing from the scope of the present invention as defined by the following claims.

What is claimed is:

1. A method for transmitting packet data in a radiocommunication system comprising the steps of:

storing, by a base station, data associated with a mobile station from a first packet data transaction;

receiving, from said mobile station, a packet for starting a second packet data transaction;

determining, by said base station, whether said packet has been correctly received;

correlating said stored data with at least one field in said packet; and

reserving, by said base station, a resource for transmission of at least one subsequent packet from said mobile

station regardless of whether said packet has been correctly received if said step of correlating verifies an identity of said mobile station.

2. The method of claim 1, wherein said step of storing data stored a mobile identification number field.

3. The method of claim 1, wherein said step of determining is based on a checksum value.

4. The method of claim 1, wherein step of reserving said resource assigns at least one time slot.

5. The method of claim 1, wherein said step of receiving receives said packet during a fast page mode time slot.

6. The method of claim 1, said method further comprising the step of:

transmitting, by said base station, a transmission opportunity message to said mobile station, wherein said packet from said mobile station is received in response to said transmission opportunity message.

7. The method of claim 6, wherein said transmitting step transmits said transmission opportunity message in an active mode.

8. The method of claim 6, wherein said transmitting step transmits said transmission opportunity message in a fast page mode.

9. The method of claim 6, wherein said transmitting step transmits said transmission opportunity message while said mobile station is in a sleep mode.

10. A method for reducing the delay of the transmission of packet data comprising:

receiving a packet, said packet including a first portion, a second portion, and a packet type field said second portion including a checksum;

decoding the contents of the packet;

verifying the accuracy of the contents based on said checksum;

comparing said first portion of said packet with a stored portion if said verifying step indicates an error in the decoding step; and

assigning a time slot for the receipt of an additional packet if said first portion matches said stored portion.

11. The method of claim 10, wherein said first portion and said stored portion include a mobile identification number field.

12. The method of claim 10, wherein said first portion and said stored portion include at least one of a mobile station capability field and a modulation proposal field.

13. The method of claim 10, wherein said comparing step compares said first portion and said packet data field with said stored portion.

14. The method of claim 10, wherein said packet is received in a first mode and wherein said time slot is assigned for a second mode.

15. The method of claim 14, wherein said first mode is a fast page mode and wherein said second mode is an active mode.

16. The method of claim 10, wherein said first portion and said stored portion each comprise a predetermined number of bits, said comparing step further comprising:

comparing each bit of said first portion with said second portion,

indicating that said first portion matches said second portion if a respective predetermined number of bits match from said first portion and said second portion.

17. A base station comprising:

a transceiver for receiving a data packet from a mobile station, said data packet including a first portion, a second portion, and a packet type field;

decoding the means for decoding contents of the packet;

verifying means for verifying the accuracy of the contents based on a checksum; and

a processor for comparing said first portion of said data packet with a stored portion if said verifying means indicates an error in the decoding of the packet contents,

wherein said processor assigns a time slot for the receipt of an additional packet if said first portion matches said stored portion.

18. The base station of claim 17, wherein said first portion and said stored portion comprise a mobile identification number field.

19. The base station of claim 17, wherein said first portion and said stored portion comprise at least one of a mobile station capability field and a modulation proposal field.

20. The base station of claim 17, wherein said processor compares said packet type field and said first portion with said stored portion.

21. The base station of claim 17, wherein said second portion includes a checksum.

* * * * *

24/3,K/20 (Item 20 from file: 350)
DIALOG(R)File 350:Derwent WPIX

009231435 **Image available**
WPI Acc No: 1992-358855/199244
XRPX Acc No: N92-273520
Zoned mobile radio **communication system - assigns tenant identifications to all** radio **terminals such that connection to line controller is selectively enabled according to service area**
Patent Assignee: NEC CORP (NIDE)
Inventor: KOJIMA S
Number of Countries: 009 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 510630	A2	19921028	EP 92106931	A	19920423	199244 B
AU 9215056	A	19921029	AU 9215056	A	19920423	199251
JP 4324724	A	19921113	JP 91122581	A	19910424	199252
CA 2066864	A	19921025	CA 2066864	A	19920422	199303
AU 652041	B	19940811	AU 9215056	A	19920423	199435
EP 510630	A3	19931118	EP 92106931	A	19920423	199512
US 5438608	A	19950801	US 92873227	A	19920424	199536
			US 94213455	A	19940314	
CA 2066864	C	19990119	CA 2066864	A	19920422	199914

Priority Applications (No Type Date): JP 91122581 A 19910424
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 510630	A2	E	11	H04Q-007/04	
Designated States (Regional): DE GB IT NL SE					
JP 4324724	A		5	H04B-007/26	
AU 652041	B			H04B-007/26	Previous Publ. patent AU 9215056
US 5438608	A		11	H04Q-007/38	Cont of application US 92873227
AU 9215056	A			H04B-007/26	
CA 2066864	A			H04B-007/26	
EP 510630	A3			H04Q-007/04	
CA 2066864	C			H04B-007/26	

Zoned mobile radio **communication system**...

...**assigns tenant identifications to all** radio **terminals such that connection to line controller is selectively enabled according to service area**

...Abstract (Basic): The communication area is divided into a number of **radio** zones, each with a **radio** base station connected to a line controller linked to subscriber lines. **Radio** terminals communicate with the base stations, both having stored tennant identification data. Before any **radio** channel is set up a **radio** terminal transmits its tenant identification to the base station...

...employed, such that a given zone may be designated a common zone in which all **radio** terminals may operate. A selected **radio** terminal may also be recognised in all zones...

...USE - Provides **radio** communication system capable of limiting service area, esp. on company basis...
...Abstract (Equivalent): The cordless telephone or similar **radio** communication system has a service area divided into a number of **radio** zones and comprises a **radio base station assigned** to each of the **radio** zones and connected to a line controller connected to

subscriber lines which extend from a public switched telephone network, and a number of **radio** terminals connectable to the **radio** base station over a **radio** channel. The **radio** base station and **radio** terminals **each** comprises a tenant **identification** (**ID**) data storage for storing tenant ID data...

...The **radio** terminals each comprise a tenant ID data transmitting section for transmitting, before the **radio** channel is set up, the tenant ID data read out of the tenant ID data storing section to the **radio** base station. The **radio** base station comprises a **radio** channel connecting section for comparing the received tenant ID data with the tenant ID data **assigned** to the **radio** **base** **station** and,if the two tenant ID data are identical, setting up the **radio** channel...

...USE/ADVANTAGE - Limits service available for **mobile** unit or **radio** terminal in exclusive zone assigned to terminal and removes limitation in common zone while opening all zones to particular **radio** terminal. All terminals belonging to respective companies are serviced at restaurant, lobby or similar common...

...Title Terms: **MOBILE** ;

US005438608A

United States Patent [19]

Kojima

[11] Patent Number: 5,438,608

[45] Date of Patent: Aug. 1, 1995

[54] **MOBILE RADIO COMMUNICATION SYSTEM HAVING BASE STATIONS AND RADIO TERMINALS EACH HAVING TENANT IDENTIFICATION DATA STORAGE FOR STORING TENANT ID DATA**

[75] Inventor: **Susumu Kojima**, Tokyo, Japan

[73] Assignee: **NEC Corporation**, Tokyo, Japan

[21] Appl. No.: **213,455**

[22] Filed: **Mar. 14, 1994**

Related U.S. Application Data

[63] Continuation of Ser. No. 873,227, Apr. 24, 1992, abandoned.

[30] **Foreign Application Priority Data**

Apr. 24, 1991 [JP] Japan 3-122581

[51] **Int. Cl.**[6] **H04Q 7/38**

[52] **U.S. Cl.** **379/58**; 379/59; 379/62; 455/33.2; 455/56.1

[58] **Field of Search** 370/95.1; 379/56, 58, 379/60, 62, 59; 455/33.1, 33.4, 33.2, 56.1

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,467,141	8/1984	Resch et al.	379/62
4,833,702	5/1989	Shitara et al.	379/60
4,852,148	7/1989	Shibata et al.	379/59
4,881,271	11/1989	Yamauchi et al.	455/56.1
5,020,094	5/1991	Rash et al.	379/62

FOREIGN PATENT DOCUMENTS

0344989	12/1989	European Pat. Off. .	
0388034	9/1990	European Pat. Off. .	
3738829	5/1989	Germany .	
0317035	12/1989	Japan	455/33.2
3219795	9/1991	Japan	379/58
2166622	5/1986	United Kingdom .	

OTHER PUBLICATIONS

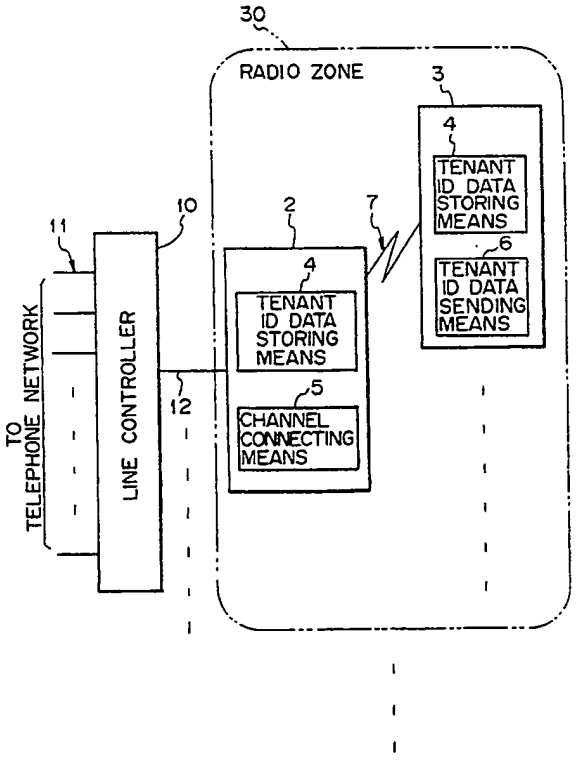
Patent Abstracts of Japan, vol. 15, No. 502, 18 Dec. 1991.

Primary Examiner—Curtis Kuntz
Assistant Examiner—William Cumming
Attorney, Agent, or Firm—Sughrue, Mion, Zinn, Macpeak & Seas

[57] **ABSTRACT**

A cordless telephone system or similar mobile radio communication system which limits the service available for a mobile unit or radio terminal in an exclusive zone assigned to the terminal and removes the limitation in a common zone while opening all the zones to a particular radio terminal. Assuming a single building accommodating a plurality of companies, the area where radio terminals can be serviced is limited on a companay basis. All the terminals belonging to the respective companies are serviced at a restaurant, lobby or similar common space inside the building. An exclusive terminal for a guard, for example, is serviced in all the arears inside the building.

3 Claims, 7 Drawing Sheets



serviced on a company basis, allows all the terminals belonging to respective companies to be serviced at a restaurant, lobby or similar common space, and allows an exclusive terminal for a guard, for example, to be serviced in all the arears inside the building.

Various modifications will become possible for those skilled in the art after receiving the teachings of the present disclosure without departing from the scope thereof.

What is claimed is:

1. A mobile radio communication system having a service area divided into a plurality of radio zones and comprising a radio base station assigned to each of said plurality of radio zones, each of said radio base stations being connected to a line controller which is connected to subscriber lines which extend from a public switched telephone network, and a plurality of radio terminals which are connected to said radio base stations over a radio channel, said radio base stations each comprising first tenant identification (ID) data storing means for storing first tenant ID data, said first tenant ID data indicating at least one service group of said radio terminals, and said radio terminals each comprising second tenant ID data storing means for storing second tenant ID data, said second tenant ID data indicating a particular one of said service groups to which the radio terminals belong;

said radio terminals each comprising tenant ID data transmitting means for transmitting, before a connection of a radio channel is set up, the second tenant ID data, read out of said second tenant ID data storing means, to said radio base station;

each of said radio base stations comprising radio channel connecting means for comparing the second tenant ID data received from said tenant ID data transmitting means of a particular one of said radio terminals with the first tenant ID data stored in said first tenant ID data storing means thereof and, if the first and second tenant ID data are identical, said radio channel connecting means causes a setting means to set up a connection of the radio channel between an associated one of said base stations and a particular one of said radio terminals, if the first and second tenant ID data are not identical, said radio channel connecting means prohibits a connection of the radio channel between the associated one of said base stations and the particular one of said radio terminals.

2. A mobile radio communication system as claimed in claim 1, further comprising:

first executing means for causing said setting means to set up a radio channel connection if the second tenant ID data received from one of said second tenant ID data storing means of said radio terminals has a first predetermined value; and

second executing means for causing said setting means to set up a radio channel connection if the first tenant ID data stored in said first tenant identification data storing means associated with said radio base station has a second value.

3. A system as claimed in claim 1 wherein one common control channel is serviced for each of said radio terminals.

* * * * *

24/3,K/24 (Item 24 from file: 347)
DIALOG(R)File 347:JAPIO

05768734 **Image available**
BASE STATION SELECTION METHOD

PUB. NO.: 10-051834 [JP 10051834 A]
PUBLISHED: February 20, 1998 (19980220)
INVENTOR(s): TAKAHASHI MASAHIRO
NAKAMURA OSAMU
TAKANASHI HITOSHI
APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT> [000422] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-206230 [JP 96206230]
FILED: August 05, 1996 (19960805)

BASE STATION SELECTION METHOD

ABSTRACT

PROBLEM TO BE SOLVED: To provide a **base station selection** method capable of reducing the number of times of hand-over than as before...

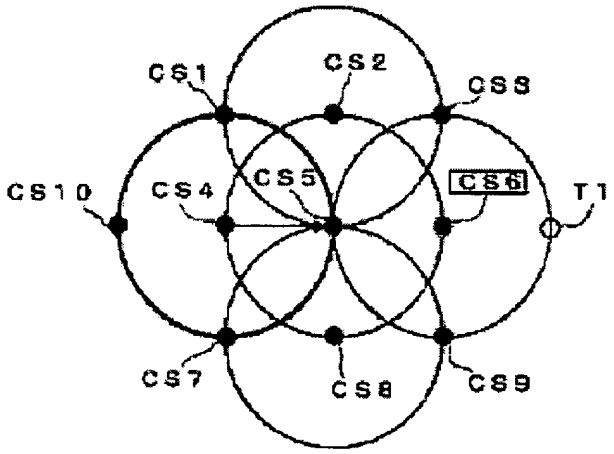
...SOLUTION: On the way of movement of a **mobile** station from a base station CS4 in the direction of a base station CS6 through a **radio** zone, in the case that hand-over is applied to a cell end (position of CS5) of the base station CS4, the **mobile** station compares **each** newest base station **identifier** (CD- **ID** of CS 2, 4, 5, 6, 8) included in an outgoing control signal with **each** base station **identifier** (CS- **ID** of CS1, 4, 5, 7, 10) stored at a preceding time and the collated base station identifier (CS-ID 4, 5) from a **base station selection** list and a **base station** CS6 where a reception level of an outgoing signal is monotonously increased and whose reception level is lowest is **selected** as a hand-over destination **base station** among the base stations whose identifier (CS-ID 2, 6, 8) left in the **base station selection** list.

BASE STATION SELECTION METHOD

Patent number: JP10051834
Publication date: 1998-02-20
Inventor: TAKAHASHI MASAHIRO; NAKAMURA OSAMU; TAKANASHI HITOSHI
Applicant: NIPPON TELEGRAPH & TELEPHONE
Classification:
- international: ***H04Q7/22;*** **H04Q7/22**; (IPC1-7): H04Q7/22
- european:
Application number: JP19960206230 19960805
Priority number(s): JP19960206230 19960805

Abstract of **JP10051834**

PROBLEM TO BE SOLVED: To provide a base station selection method capable of reducing the number of times of hand-over than as before. SOLUTION: On the way of movement of a mobile station from a base station CS4 in the direction of a base station CS6 through a radio zone, in the case that hand-over is applied to a cell end (position of CS5) of the base station CS4, the mobile station compares each newest base station identifier (CD-ID of CS 2, 4, 5, 6, 8) included in an outgoing control signal with each base station identifier (CS-ID of CS1, 4, 5, 7, 10) stored at a preceding time and the collated base station identifier (CS-ID 4, 5) from a base station selection list and a base station CS6 where a reception level of an outgoing signal is monotonously increased and whose reception level is lowest is selected as a hand-over destination base station among the base stations whose identifier (CS-ID 2, 6, 8) left in the base station selection list.



31/3,K/49 (Item 49 from file: 347)
DIALOG(R)File 347:JAPIO

05422538 **Image available**
CHANNEL SETTING CONTROL SYSTEM

PUB. NO.: 09-037338 [JP 9037338 A]
PUBLISHED: February 07, 1997 (**19970207)**
INVENTOR(s): KURIAKI SHINICHI
APPLICANT(s): FUJITSU LTD [000522] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 07-185562 [JP 95185562]
FILED: July 21, 1995 (19950721)

...PUBLISHED: **19970207)**
INTL CLASS: **H04Q-007/36**

ABSTRACT

... under an existing number plan in respect to a channel setting control system for a **mobile** communication system...

...SOLUTION: This channel setting control system is provided with a **base station** 11 for sending a number applied by an incoming call **selection** signal through an inter-station signal line to a **radio** zone and controlling the channel setting of **mobile** stations in the **radio** zone and **plural mobile** stations 12(sub 1) to 12(sub n) **each** of which compares the number sent from the **base station** 11 with a **mobile** station number previously allocated to the station itself, and when both the numbers coincide with **each** other, receiving communication service based upon a channel setting control procedure. **Each** slave station 12 is provided with a call detection control means 13 including the **identification** (**ID**) numbers of **base stations** forming the **radio** zone in which the station itself can receive communication service and using a **unique** annexed **mobile** station number allocated to the station itself as a comparing object and the ID number of the **base station** 11 is allocated to an inter-station signal line as an office number.

CHANNEL SETTING CONTROL SYSTEM

Patent number:	JP9037338
Publication date:	1997-02-07
Inventor:	KURIAKI SHINICHI
Applicant:	FUJITSU LTD
Classification:	
- international:	***H04Q7/36;*** **H04Q7/36**; (IPC1-7): H04Q7/36
- european:	
Application number:	JP19950185562 19950721
Priority number(s):	JP19950185562 19950721

Report a data error here

Abstract of **JP9037338**

PROBLEM TO BE SOLVED: To inexpensively and surely apply a direct dialing system under an existing number plan in respect to a channel setting control system for a mobile communication system. SOLUTION: This channel setting control system is provided with a base station 11 for sending a number applied by an incoming call selection signal through an inter-station signal line to a radio zone and controlling the channel setting of mobile stations in the radio zone and plural mobile stations 121 to 12n each of which compares the number sent from the base station 11 with a mobile station number previously allocated to the station itself, and when both the numbers coincide with each other, receiving communication service based upon a channel setting control procedure. Each slave station 12 is provided with a call detection control means 13 including the identification(ID) numbers of base stations forming the radio zone in which the station itself can receive communication service and using a unique annexed mobile station number allocated to the station itself as a comparing object and the ID number of the base station 11 is allocated to an inter-station signal line as an office number.